



AUSTRALIAN  
**CRIMINAL  
INTELLIGENCE  
COMMISSION**

# SERIOUS FINANCIAL CRIME IN AUSTRALIA **2017**



# CONTENTS

<b>FOREWORD .....</b>	<b>6</b>
<b>INTRODUCTION .....</b>	<b>8</b>
Defining serious financial crime .....	8
Tackling serious financial crime .....	9
Generating financial crime intelligence .....	11
<b>FINANCIAL CRIME ENABLERS .....</b>	<b>12</b>
Money laundering .....	12
Technology .....	14
Identity crime .....	15
Professional facilitators .....	17
Offshore service providers .....	19
Illegal phoenix activity .....	21
Abusive use of trusts .....	23
High-value commodities .....	25
Alternative banking services .....	27
<b>FINANCIAL CRIME MARKETS .....</b>	<b>28</b>
Cybercrime .....	28
Investment and financial market fraud .....	30
Revenue and taxation fraud .....	34
Superannuation fraud .....	37
Card fraud .....	39
Health and welfare fraud .....	43
<b>FINANCIAL CRIME OUTLOOK IN AUSTRALIA .....</b>	<b>45</b>
Key predictions .....	45
Opportunities .....	45
<b>ACRONYMS .....</b>	<b>47</b>

# SNAPSHOT



## MONEY LAUNDERING

‘Money laundering occurs on a global scale with proceeds of crime transferred between jurisdictions, commingled with legitimate monies and integrated into legitimate markets.’



## TECHNOLOGY

‘As the rapid uptake of technology and the online environment grows, criminal groups and individuals exploit this as means to commit, facilitate or conceal criminality.’



## IDENTITY CRIME

‘Identity crime, although under-reported, is now among the most prevalent and constantly changing crime types.’



## PROFESSIONAL FACILITATORS

‘Increasingly, the globalised and complex nature of the financial sector, and the legislative and regulatory rules that govern it, make it necessary to engage professionals with specialist knowledge and skills.’



## OFFSHORE SERVICE PROVIDERS

‘The anonymity afforded to clients of an OSP enables a range of criminal activity, including money laundering, and investment, superannuation and taxation fraud.’



## ILLEGAL PHOENIX ACTIVITY

‘Illegal phoenix activities divert money that should be afforded to the Australian revenue and tax systems to criminal individuals through their businesses.’



## ABUSIVE USE OF TRUSTS

‘Criminal groups and individuals use trust funds to conceal criminal wealth, support criminal activity and launder illicit funds.’



## HIGH VALUE COMMODITIES

‘Precious gems and metals, art and antiquities ... present opportunities for organised crime and criminal entities to transfer and store illicit wealth.’



## ALTERNATIVE BANKING SERVICES

‘Alternative Banking Services (ABS) are used by individuals and companies to move funds around the world outside existing regulated banking frameworks.’



### **CYBERCRIME**

'The global cybercrime market is a low risk, high return criminal enterprise.'



### **INVESTMENT AND FINANCIAL MARKET FRAUD**

'Australia will continue to be a target for domestic and offshore investment fraud activities.'



### **REVENUE AND TAXATION FRAUD**

'Identity crime related to refund fraud is an increasing problem.'



### **SUPERANNUATION FRAUD**

'Australia's large pool of superannuation funds is an attractive target for criminal groups and individuals.'



### **CARD FRAUD**

'The rise in card-not-present fraud correlates with the increase in popularity of online shopping and the associated increase in the storage of these details online.'



### **HEALTH AND WELFARE FRAUD**

'...it is anticipated that the targeting of online government portals will increase and that these systems may possibly be breached by offshore entities.'

# **WORLDWIDE, FINANCIAL CRIME IS ON THE RISE**

# FOREWORD

Serious Financial Crime in Australia 2017 is the inaugural unclassified report produced by the Australian Criminal Intelligence Commission that highlights the way serious financial crimes are impacting on the Australian community.

As a member agency of the Serious Financial Crime Taskforce, the Australian Criminal Intelligence Commission is responsible for assessing the financial crime threat picture. To do this, we collaborate with government partners, industry and the community to collect information and intelligence that inform these threat assessments and appropriate response strategies.

Serious financial crime impacts on all Australians. For some, it may be the direct loss of savings through an investment scam, or the compromise of their personal information, which is then used to commit credit card fraud.

For most, it is the indirect impacts of serious financial crime that are less obvious but more wide-ranging. For example, the loss of government revenue resulting from tax fraud and health and welfare fraud means there are fewer funds available to the government to spend on essential services such critical infrastructure, health and welfare benefits and education programs.

Serious financial crime threats are located both in Australia and offshore. We estimate that around 70 per cent of Australia's serious and organised criminal threats are based offshore or have strong offshore links. As a result, the Australian Criminal Intelligence Commission has been building closer relationships with international partners to facilitate knowledge-sharing of transnational crime threats, including serious financial crime threats that are impacting on Australia. This supports us in building more accurate threat assessments and informs effective response strategies.

Serious financial crime is committed by serious and organised crime groups and criminal entrepreneurs who have the expertise and resources—similar in some ways to the traditional 'white collar' criminals. However, the way in which financial crime is committed has evolved significantly compared to the traditional methods of the past.

Technology is playing an increasingly significant role in enabling financial crime. For example, technology has enabled large-scale phishing and targeted data hacks to obtain personal identifying information, which can then be used to facilitate other financial crimes such as card fraud.

We are also seeing an increase in cybercrime intrusions into superannuation and payroll platforms that contain a range of personal and financial information that could be used to enable further criminal activities.



The threat posed by technology-enabled financial crime and cybercrime activities will continue to grow as technology evolves and as government and industry continue to integrate technology into service delivery.

The complexity of financial crime is also increasing. The expertise of professional facilitators who help to navigate financial frameworks and technology systems to exploit vulnerabilities often makes it difficult to even identify that a crime has been committed. This proficiency is extremely valuable to individuals and groups wanting to test framework boundaries, exploit systemic vulnerabilities, or to circumvent laws and commit criminal acts. Professional facilitators play a fundamental role in navigating financial, regulatory and information systems to support financial crime.

Offshore service providers are also playing an increasing, more visible role in assisting tax evasion or, in some cases, laundering the proceeds of crime.

All of these factors—offshore threats, technology and professional facilitators—contribute to the complexity of financial crime affecting Australia.

The Australian Criminal Intelligence Commission was formed to strengthen our response to crime affecting Australia. Through our investigative, research and information delivery services, we are actively working with our law enforcement partners to stop criminals exploiting emerging opportunities and perceived gaps in law enforcement information.

As serious financial crime in Australia increases, so too do our law enforcement and intelligence capabilities to combat serious and organised crime. Through our Determination Targeting Criminal Wealth No. 2 Special Investigation, we are actively monitoring financially-motivated crime, working to disrupt and deter criminal groups, collecting evidence and intelligence about their illicit activities and connecting our law enforcement partners to this crucial information.

This special investigation into financially-motivated crime brings together our work investigating money laundering, serious and organised investment fraud, sophisticated tax evasion and confiscating criminal wealth. It enables us to work with our partners to:

- deliver financial intelligence that identifies high-value targets and provides new opportunities for law enforcement and regulatory partners
- build national knowledge of money laundering, nationally significant tax fraud and other financially-motivated crimes
- help make Australia unattractive for abusive financial arrangements and money laundering
- reduce the impact of serious financial crime on the Australian community
- produce intelligence that contributes to whole-of-government policies and law enforcement decision-making.

Our mission is to make Australia safer through an improved national ability to discover, understand and respond to current and emerging crime threats and criminal justice issues, including the ability to connect police and law enforcement to essential policing knowledge and information. By building a national threat picture, we can inform government partners, industry participants and the community about key threats, strategies to disrupt crime and opportunities to better position ourselves against emerging threats.



Michael Phelan APM  
Chief Executive Officer  
Australian Criminal Intelligence Commission

# INTRODUCTION

*Serious Financial Crime in Australia 2017* presents the national picture of serious financial crime currently impacting on the Australian community.

In 2015, the Australian Government established the Serious Financial Crime Taskforce, a multi-agency task force that unites the operational and strategic intelligence capacity and responsibilities of task force agencies to identify and respond to serious financial crime in Australia. The Serious Financial Crime Taskforce member agencies include:

- Attorney-General's Department (AGD)
- Australian Border Force (ABF)
- Australian Criminal Intelligence Commission (ACIC)
- Australian Federal Police (AFP)
- Australian Securities and Investments Commission (ASIC)
- Australian Taxation Office (ATO)
- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- Commonwealth Director of Public Prosecutions (CDPP).

*Serious Financial Crime in Australia 2017* draws on the collaborative work of the Serious Financial Crime Taskforce agencies, as well as intelligence and operational data held by a broad range of law enforcement, regulatory and other government agencies. The work undertaken by the Serious Financial Crime Taskforce identifies the key threat priorities for operational treatment, ongoing intelligence collection and proposed policy and legislative change. The current priorities of the Serious Financial Crime Taskforce include international tax evasion, illegal phoenix activity, abusive use of trust structures, and criminality related to offshore service providers and superannuation funds.

The objective of the Serious Financial Crime Taskforce is to maintain integrity and community confidence in the Australian economy, financial markets, regulatory framework and revenue collection.

As at August 2017, the efforts of the Serious Financial Crime Taskforce have recouped \$152.53 million for the Commonwealth, raised \$391.93 million in tax liabilities, executed 54 search warrants, completed 587 audits, prosecuted four people and convicted four people.<sup>1</sup>

## DEFINING SERIOUS FINANCIAL CRIME

Financial crime causing major harm to Australia extends beyond that being committed by serious and organised crime groups. In particular, a significant and growing threat is presented by sophisticated individuals and groups exploiting systemic vulnerabilities in taxation and revenue systems and government health and welfare programs. This is in addition to individuals using offshore structures to evade paying tax in Australia.

The serious financial crime intelligence picture also highlights the complexity of some of the emerging financial crime issues, many of which require ongoing multi-agency cooperation to better understand financial crime and to develop mitigation strategies. Examples include the way in which identity crime enables financial crime and the constantly evolving challenges posed by cybercrime and technology-enabled financial crime.

The role of technology in enabling financial crime at all levels has emerged as a primary theme in *Serious Financial Crime in Australia 2017*.

---

<sup>1</sup> Australian Federal Police 2017, *Serious Financial Crime Taskforce*, viewed 2 June 2017, <[https://\\_www.afp.gov.au/what-we-do/crime-types/fraud/serious-financial-crime-taskforce](https://_www.afp.gov.au/what-we-do/crime-types/fraud/serious-financial-crime-taskforce)>.

From opportunistic tax refund fraud undertaken by individuals to the large-scale online theft of personal identifying information to enable the systematic theft of funds from investment and superannuation accounts, the use of technology enables an extensive spectrum of financial crime. This has implications for the development of systems, processes and procedures to deter and protect against technology-enabled crime, and for forward planning for the capabilities and specialist resources required to identify and investigate technology-enabled crime.

Professional facilitators remain critical enablers of financial crime, particularly serious and organised crime, with the range of professionals involved extending beyond the traditional legal and accounting facilitators to include liquidators, offshore service providers and real estate agents. This reflects the increasingly complex and globalised organised crime environment.

## TACKLING SERIOUS FINANCIAL CRIME

Identifying and targeting serious financial crime remains a priority of the Australian Government, which has established a number of key initiatives aimed at addressing serious financial crime threats and reducing the impact of serious financial crime on Australians.

The high-profile financial crime initiative Project Wickenby was established in February 2006 and operated until 30 June 2015, targeting international tax evasion and those professional facilitators who promoted or participated in the abuse of offshore secrecy arrangements to support large-scale tax evasion. As at 30 June 2015, Project Wickenby had resulted in the conviction of 46 individuals, \$2.297 billion in tax liabilities raised, \$372 million from increased voluntary compliance and \$5 million in assets recovered under Commonwealth proceeds of crime provisions.

In addition to the success of Project Wickenby, the Australian Government has continued its commitment to tackling serious financial crime in Australia, by supporting a number of collaborative initiatives since 2011 that bring together government, private sector and regulatory stakeholders to target the key financial crime threats to Australia.

### CRIMINAL ASSETS CONFISCATION TASKFORCE

The AFP-led Criminal Assets Confiscation Taskforce is a Commonwealth initiative, established in March 2011, which is dedicated to taking the profit out of crime by targeting criminals and their assets derived from unexplained wealth. The Criminal Assets Confiscation Taskforce brings together the resources of the AFP, ATO and ACIC, as an integrated approach to targeting the financial base of criminals and confiscating assets bought with proceeds of crime.

### FRAUD AND ANTI-CORRUPTION CENTRE

In 2013, the AFP-led multi-agency Fraud and Anti-Corruption Centre was established to focus on serious and complex fraud against the Commonwealth, corruption by Australian Government employees, foreign bribery and complex identity crime involving the manufacture and abuse of official credentials.

The Serious Financial Crime Taskforce forms part of the Fraud and Anti-Corruption Centre and builds on the success of offshore tax evasion work carried out under Project Wickenby. The Serious Financial Crime Taskforce has a broader remit than the Fraud and Anti-Corruption Centre. It targets the highest priority serious financial crimes and focuses on operational activities, the collection and sharing of intelligence, the identification of potential reform measures with the aim of removing wealth derived from illegal activities, prosecuting facilitators and promoters of serious financial crime and the deployment of deterrent and preventative enforcement strategies.

### TAX AVOIDANCE TASKFORCE—TRUSTS; FORMERLY TRUSTS TASKFORCE

In 2013, the ATO-led Trusts Taskforce was established to take compliance action against known tax scheme designers, promoters, individuals and businesses who have been involved in tax avoidance or evasion using trust structures. The Trusts Taskforce raised \$948 million in liabilities and collected \$279 million from individuals and businesses involved in tax avoidance or evasion using trusts. An additional \$55 million worth of assets have also been restrained under proceeds of crime legislation.

Since 1 July 2017, the work of the Trusts Taskforce has continued under the ATO's Tax Avoidance Taskforce - Trusts.

### PHOENIX TASKFORCE

Established in 2014, the Phoenix Taskforce comprises of over 20 Federal, State and Territory government agencies providing a whole-of-government approach to combating illegal phoenix activity. The Phoenix Taskforce also works in collaboration with the Serious Financial Crime Taskforce to identify and treat serious financial crime related to illegal phoenix behaviour.

The Phoenix Taskforce aims to share data and intelligence to capture both phoenix companies and those potentially aiding businesses by providing unlawful insolvency advice.

In 2015–16, the Phoenix Taskforce conducted almost 1,000 audit and review cases involving phoenix behaviour, raising \$250 million in liabilities.

### AUSTRALIAN CYBERCRIME ONLINE REPORTING NETWORK

Established in 2014, the Australian Cybercrime Online Reporting Network (ACORN) is the ACIC-led national policing initiative of the Commonwealth, state and territory governments that enables the public to securely report instances of cybercrime through a national online system. As well as facilitating the public's reporting of cybercrime events, ACORN helps the government to better understand the enablers of cybercrime so that it can educate members of the public to recognise common types of cybercrime. This increased understanding also informs response strategies that make Australian citizens less attractive for cybercriminals to target.

In the 2016–17 financial year, ACORN received 874 reports with a total estimated loss of more than \$20 million—a figure that is more than double the estimated loss of \$8.6 million reported to ACORN in the 2015–16 financial year.

### AUSTRALIAN FINANCIAL CRIMES EXCHANGE

In November 2016, the AGD-led Australian Financial Crimes Exchange was launched, partnering the ANZ, the Commonwealth Bank, the National Australia Bank and Westpac with the Australian Government to provide leading security capabilities, technology and intelligence on a centralised platform. This platform allows financial institutions to share fraud and cybercrime-related data. This aims to improve responses to these types of financial crimes and reduce the impact on customers and shareholders.

### FINTEL ALLIANCE

Launched in March 2017, the AUSTRAC-led Fintel Alliance is a public-private partnership aimed at combating money laundering and terrorism financing. The Fintel Alliance supports the real-time exchange of financial intelligence, data, tracking tools and methodologies on a global scale. The three operational goals of the Fintel Alliance are:

- to help private sector partners more easily identify and report suspicious transactions
- to help law enforcement partners more quickly arrest and prosecute criminals
- to work with academia to build knowledge and gather insight.

The United Kingdom's National Crime Agency is the first international member of the Fintel Alliance Operations Hub. With membership from Australian Government agencies, industry partners and international law enforcement, the Fintel Alliance aims to protect the integrity of Australia's financial systems from organised crime and terrorism financiers impacting on Australia.

### BLACK ECONOMY TASKFORCE

In 2017, the Australian Government established the Black Economy Taskforce, a policy response initiative to examine the practices of those who operate entirely outside the tax and regulatory system or who do not correctly report tax obligations.

Cash businesses present a variety of opportunities to launder money, including through:

- illicit funds being mingled with legitimate business earnings
- illicit funds being used to purchase stock, equipment and premises which in turn can increase the resale value of that business
- false sales records being created to inflate business turnover, which allows for the injection of illicit funds.

## GENERATING FINANCIAL CRIME INTELLIGENCE

It is difficult to quantify the annual loss of funds to financial crime committed by serious and organised crime groups and criminal individuals or the real sum lost to the Commonwealth and victims through various forms of fraud. However, what does seem apparent is that both of these financial crime impacts present important risks to Australia.

Through the work programs of these various financial crime initiatives, it is expected that a more comprehensive intelligence picture of the impact of serious financial crime on the Australian community and the disruption effects of public-private collaboration and interactive targeting efforts will be generated.

*Serious Financial Crime in Australia 2017* focuses on the 'enablers' and 'markets' of financial crime.

Enablers play a unique role in enabling or facilitating serious and organised financial crime. There are some criminal groups and individuals who specialise in one or more of these enabling activities, providing services to other individuals and groups engaged in serious financial crime.

For example, a specialised money laundering syndicate would provide a money laundering service to a group involved in organised fraud, enabling that group to move the proceeds of their fraud activities offshore. Each of the enablers can facilitate financial crime to varying extents; however, some enablers have a more fundamental role than others. Enablers can work in unison, with one crime group using several enablers concurrently.

Financial crime markets represent those markets where the participants exchange goods or services, but those goods or services are delivered or presented in an illegal, malicious or fraudulent manner. For example, criminal groups and individuals seeking to defraud the government of income tax or health and welfare benefits would misrepresent their position in order to gain additional benefits they are not entitled to or evade paying tax. Therefore, revenue and taxation fraud and health and welfare fraud are regarded as financial crimes where criminals are 'market participants' in the tax system or government programs. The financial crime markets addressed in this report reflect the highest priority markets, where the impact on Australians and the Australian economy is the most significant.



**FINANCIAL CRIMES ARE  
DIVERSE IN NATURE,  
SCALE AND THE LEVEL  
OF HARM THEY CAUSE**

# FINANCIAL CRIME ENABLERS

## MONEY LAUNDERING

### INTRODUCTION

Australia continues to sustain very profitable crime markets, such as the illicit drug market, and as a result there is a need to launder the significant proceeds that these crimes generate.

Methodologies used to launder the proceeds of drug crime, for example, are likely to differ from the methodologies used to launder the profits of financial crime. The former requires larger amounts of illegal cash to be placed into banking or alternative remittance systems before it can be laundered, while financial crime proceeds are more likely to already be in the legitimate banking systems. It is likely that the majority of the profit from financial crime is laundered by transferring funds through a series of bank accounts in different jurisdictions. Corporate structures within Australia and overseas are also used to facilitate this process.

Regardless of the source of the proceeds of crime, in order to use the illegal funds to facilitate further criminal activity or to support a lavish lifestyle, it is necessary to launder them and to obscure their criminal origins.

### CURRENT SITUATION

Money laundering remains a fundamental enabler of financial crime and is a significant and potentially lucrative criminal enterprise in itself. As well, our stable financial markets and valuable real estate market make Australia an attractive destination for criminal groups and individuals looking to invest or launder the proceeds of crime.

Money laundering occurs on a global scale with proceeds of crime transferred between jurisdictions, commingled with legitimate monies and integrated into legitimate markets. Australian law enforcement has continued to gain significant insights into the operations of transnational money laundering organisations, the methodologies used by such groups and their connections to other serious and organised crime groups.



### MONEY LAUNDERING KEY OBSERVATIONS

- Money laundering remains a fundamental enabler of financial crime and is a significant and potentially lucrative criminal enterprise in itself.
- Some organised crime groups are using more global methods to launder proceeds of crime, including using the services of transnational money laundering organisations, money mules, remittance services and trade-based money laundering.

### ALTERNATIVE REMITTANCE SERVICES

It is almost certain that groups and individuals involved in financial crime are engaging transnational money laundering organisations to launder illicit profits through alternative remittance services both in Australia and overseas.

Alternative remittance services use money transfer methodologies such as informal value transfer systems to remit a value amount without the physical transfer of cash, whether this is legitimate cash or proceeds of crime.

### SMART AUTOMATIC TELLER MACHINES

Smart automatic teller machines capable of accepting cash deposits have the potential vulnerability of allowing people to make illicit cash deposits into third-party accounts. This practice, although not entirely anonymous, has been seen as an opportunity to move cash into accounts while avoiding face-to-face interactions with bank staff members, who could identify suspicious transactions and report them.

## STORED VALUE CARDS

Above threshold stored value cards (SVCs)<sup>2</sup> have been identified as being used to move large sums of money derived from the proceeds of crime through established financial networks, often offshore.

While above threshold SVCs are subject to anti-money laundering/counter-terrorism financing reporting, below threshold SVCs<sup>3</sup> have also been identified as being used to launder money, despite holding less monetary value. Below threshold SVCs are an attractive option, though, as they offer complete anonymity and do not attract reporting obligations. The limitation of storage value is often circumvented by purchasing multiple cards.<sup>4</sup>

## TRADE-BASED MONEY LAUNDERING

Trade-based money laundering (TBML) is defined as ‘the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illegal origin or finance their activities’.<sup>5</sup>

There are a number of TBML techniques, including over- or under-invoicing, over- or under-shipment, false invoicing, and black market peso exchange. These techniques can be effectively applied either in isolation or in combination, exploiting the complex nature of trade and trade finance to conceal the movement of illicit value.

- 2 An SVC is regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* and carries reporting obligations if the card can hold \$1,000 or more at any one time and cash can be withdrawn from the card, or if the card can hold \$5,000 or more at any one time and cash cannot be withdrawn from the card.
- 3 An SVC that does not meet the relevant thresholds, as set out for above threshold SVCs, is not regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.
- 4 Australian Transaction Reports and Analysis Centre 2017, *Stored Value Cards Money Laundering and Terrorism Financing Risk Assessment*, viewed 12 April 2017, <<http://www.austrac.gov.au/sites/default/files/stored-value-cards-risk-assessment-WEB.pdf>>.
- 5 In 2008, the Financial Action Task Force’s Paper on Best Practices broadened the definition of TBML to incorporate the use of TBML methodologies for terrorist financing. Financial Action Taskforce 2008, *Best Practices Paper on Trade Based Money Laundering*, FATF/OECD, France, viewed 12 April 2016, <<http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf>>.

## ONLINE WAGERING PLATFORMS

Serious and organised crime entities may have both access to and control of offshore wagering platforms. Betting activity through offshore platforms also conceals betting activity on corrupted sports and racing events, and the potential laundering of criminal wealth.

## USE OF COMPLEX OFFSHORE BUSINESS STRUCTURES

Money laundering methodologies can, and frequently are, combined with the use of offshore corporate entities to further obscure the criminal origin of such funds. The recent exposure of Mossack Fonseca client information provides insight into the ease with which offshore companies and associated bank accounts can be created in multiple jurisdictions and used to electronically transfer illicit funds around the world.

## PROFESSIONAL FACILITATORS

In order to set up the structures needed to launder the profits of financial crime, serious and organised crime groups and criminal individuals almost certainly use a range of professional facilitators, both within Australia and offshore. Members of serious and organised crime groups involved in financial crime are likely to have a degree of financial literacy and knowledge of the types of structures required to conceal their involvement in such criminal activity. However, the creation and maintenance of these structures almost certainly requires the use of professional facilitators.

## OUTLOOK

The electronic transfer of funds to multiple accounts in different jurisdictions is likely to remain the dominant method used to launder the proceeds of financial crime. However, transnational money laundering organisations, money mules and remittance services have been identified as being used by serious and organised crime groups involved in financial crime. These trends are likely to continue but will change, and methodologies will be displaced as continued success in law enforcement targeting of particular methodologies occurs.

The ability of those involved in serious and organised crime to launder money allows for re-investment, and therefore the perpetuation of criminal enterprises. Money laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment, distort international capital flows and damage diplomatic relations.

Further harm may be caused by the methods with which money laundering occurs. The primary goal of money laundering is to give illicitly-derived money the appearance of legitimacy. Consequently, funds are likely to be invested not on the basis of likely returns, but in businesses or schemes that provide the greatest chance of concealing the origins of the money. This can erode the 'level playing field' on which legitimate businesses compete, distort markets, and enhance the economic power of organised crime.

## TECHNOLOGY

### INTRODUCTION

Technology has enabled organised crime and has provided criminals engaging in financial crime with ready access to a significantly larger number of potential victims, personal identifying information and victim funds. Organised crime groups frequently seek out individuals skilled in the use of technology to enable them to target victims of financial fraud including card fraud, investment fraud and superannuation fraud.

The use of technology in facilitating financial crime is particularly attractive as it enables criminal groups and individuals to identify and target significantly larger groups of potential victims from any location in the world, while expending few resources. Similarly, the use of technology in financial crime can obscure the identity and location of criminal groups and individuals, which makes it a low risk activity with a potential for high return.

### CURRENT SITUATION

The use of technology to enable financial crime has grown steadily over the past 10 years in line with advancements in the accessibility and variety of available technology and financial platforms. As the rapid uptake of technology and the online environment grows, criminal groups and individuals exploit this as means to commit, facilitate or conceal criminality.



## TECHNOLOGY KEY OBSERVATIONS

- The use of technology to enable financial crime has increased significantly over the past two years, with the most serious financial crime now enabled by technology. It is almost certain that this increase will continue over the next two years.
- Those who possess specialist information and communications technology skills are almost certain to play an increasingly important role in supporting the activities of groups and individuals who intend to commit serious financial crimes.

The anonymity offered by virtual currencies and associated software applications is likely to be highly attractive to criminals. Bitcoin offers a level of anonymity for users that can be increased when it is used in combination with anonymising software. There are also a range of other virtual currencies, such as ZCash and Monero, which offer anonymity far exceeding that of Bitcoin.

The increased use of technology in the financial services sector provides clients with user-friendly access to a range of products. However, this also exposes an increasing number of individuals and businesses to a range of technology-enabled financial crimes. For example, online interfaces can be copied by organised crime groups and individual fraudsters, and receive redirected traffic so victims believe they are visiting a legitimate website. This creates the opportunity to target a large number of potential victims around the world.

As technology-enabled financial crime grows, professionals who possess high-level skills in information and communications technology (ICT) are almost certain to play integral roles in facilitating financial crimes.

Open-source information provides examples of networks of ICT specialists collaborating with others who possess knowledge of financial markets.<sup>6</sup>

Individuals, businesses, government and industry who rely on or are increasing the integration of technology in service delivery are particularly vulnerable. They will need to employ requisite technical expertise, cybersecurity practices and information security infrastructure to withstand and respond to the threat of technology-enabled financial crime.

## OUTLOOK

Rapid advances in technology have provided organised crime groups and 'tech-savvy' criminal individuals with new ways to target larger pools of victims with fewer resources and less risk of detection. It is almost certain that such groups and individuals will continue to use technology to enable financial crime as well as develop new methodologies to target further victims. It is almost certain that these criminal groups and individuals will increasingly exploit the use of ICT to facilitate financial crimes and seek out professional facilitators who possess the necessary knowledge to support technology-enabled financial crime.

## IDENTITY CRIME

### INTRODUCTION

Identity crime, although under-reported, is now among the most prevalent and constantly changing crime types. As well as enabling crime, it is also a crime in its own right, carried out by serious and organised crime groups and cybercriminals.

An increased reliance on personal identifying information (PII) for online services, along with the exploitation of technology by criminals, has seen identity crime become one of the most pervasive crime types in Australia.



### IDENTITY CRIME KEY OBSERVATIONS

- The theft, and subsequent on-selling, of personal identifying information is a highly lucrative crime that can enable other serious financial crimes such as superannuation fraud and refund fraud.
- Identity crime, particularly the harvesting of personal identifying information, is likely to increase as this data is increasingly stored online.

### CURRENT SITUATION

Criminal actors employ a variety of methodologies to gain access to PII, from the theft of sensitive documentation, to more sophisticated techniques that rely on the use of technology and cybercrime techniques such as phishing,<sup>7</sup> social engineering<sup>8</sup> or the deployment of credential harvesting malware. PII is a valuable commodity, traded and sold by criminals to serious and organised crime groups with a view to facilitating other financial crimes.

### REFUND FRAUD

Refund fraud is characterised by the submission of false income tax returns or activity statements with the aim of fraudulently obtaining refunds. Organised crime groups and individuals use a range of methods to achieve this, from using a false identity or, increasingly, using stolen information to impersonate someone else.

6 Vengerik, B Dennesen, K, Berry J & Wrolstad, L 2014, *Hacking the street? FIN4 likely playing the market*, FireEye, California, viewed 15 May 2016, <[https://\\_www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf](https://_www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf)>.

7 Phishing refers to identity theft tactics surrounding email and internet use.

8 Social engineering is the use of deception to manipulate individuals into revealing PII that may be used for fraudulent purposes.

# CASE STUDY

## SUPERANNUATION-RELATED IDENTITY THEFT

A serious and organised cybercrime group hacked a superannuation fund member's home computer system, gaining access to PII including emails, banking details and travel plans. Post-hack, the group was also able to monitor the victim's superannuation fund transactions. When the victim travelled overseas the group made an online request from the victim's email for a superannuation payment variation.

The superannuation fund called the victim's contact number to confirm the variation request. However, the serious and organised crime group had diverted the victim's phone number to one it controlled. In this instance the fraud was able to be stopped after the victim noticed unusual transactions and changes on their bank account statement and the funds were frozen by the victim's bank.



**AUSTRALIA'S LARGE POOL  
OF SUPERANNUATION  
FUNDS IS ATTRACTIVE  
TO CRIMINALS**

In the 2014-15 financial year, the ATO identified and prevented incorrect refund payments valued at approximately \$754 million<sup>9</sup> out of a total legitimate refund pool of \$95 billion.

### SUPERANNUATION FRAUD

Australia's large pool of superannuation funds is an attractive target for criminals. Identity crime enables superannuation fraud through the illegal acquisition of PII that is then used to fraudulently access superannuation funds. Increasingly, technology and cybercrime techniques are facilitating illegal access to PII and are also supporting superannuation fraud activities.

Superannuation fraud in Australia is made possible through the use of technology, cybercrime techniques and identity crime. Historically, identity crime enabled fraud targeting superannuation accounts was conducted by criminal entities stealing statements from the mail and using the PII contained in these statements to create fake identity documents that were then used to steal funds. Now criminal entities are using online methods to enable fraudulent access to superannuation accounts.

### OUTLOOK

Identity crime will likely increase in frequency as the volume of PII stored online increases. As more financial services are provided online, there is a requirement for more personal identifiers, such as personal identification numbers, passwords, access codes and security questions, to be created and stored. These personal identifiers are of value to criminal entities and will continue to be harvested, sold and used in fraud and to access systems for other criminal purposes.

Identity takeover is likely to emerge as the primary identity crime methodology used to facilitate financial crime, rather than identity creation. As government agencies and private institutions increase services offered online, it is likely that new identity crime enabled financial crime methodologies will be observed.

<sup>9</sup> The ATO advises that there can be difficulties quantifying refund fraud as there are sometimes difficulties in distinguishing between refund fraud, which is intentional, and refund integrity matters, which are unintentional.

## PROFESSIONAL FACILITATORS

### INTRODUCTION

Professional facilitators are industry professionals and subject matter experts who provide their specialist skills and knowledge, either wittingly or unwittingly, for the benefit of individuals and groups looking to engage in serious financial crime activities.

Professional facilitators may or may not be complicit in assisting criminal groups and individuals in financial crime. Some professional facilitators are unknowingly involved, some are recruited through extortion or intimidation, and others willingly participate, often making significant personal financial gains from the association.

### CURRENT SITUATION




























Increasingly, the globalised and complex nature of the financial sector, and the legislative and regulatory rules that govern it, make it necessary to engage professionals with specialist knowledge and skills. As such, professional facilitators—and the employees of professional facilitators, who also have specialist knowledge and/or access to restricted data—are attractive resources for those seeking to engage in serious financial crime.



### PROFESSIONAL FACILITATORS KEY OBSERVATIONS

- Professional facilitators are intrinsic enablers of serious financial crime, with the range of professions used to facilitate financial crime extending beyond those traditionally considered to be exploited such as lawyers and accountants, to include real estate agents, liquidators and financial advisers. Australia's current anti-money laundering/counter-terrorism financing controls are yet to reflect this diversity, creating significant opportunities for these facilitators to enable the movement of funds without the requirement to report to authorities.

**TABLE 1: PROFESSIONAL FACILITATORS INVOLVED IN SIGNIFICANT FINANCIAL CRIME ACTIVITIES**

	LAWYERS	ACCOUNTANTS/ FINANCIAL ADVISERS	LIQUIDATORS/ PRE-INSOLVENCY ADVISERS	OFFSHORE SERVICE PROVIDERS	ICT PROFESSIONALS	REAL ESTATE AGENTS
MONEY LAUNDERING						
SUPERANNUATION FRAUD						
INVESTMENT AND FINANCIAL MARKET FRAUD						
REVENUE AND TAX FRAUD						
ILLEGAL PHOENIX BEHAVIOUR						
ABUSIVE USE OF TRUSTS AND COMPANIES						
TECHNOLOGY-ENABLED FINANCIAL CRIME						

Some of the primary professional facilitators identified across some of the key financial crime markets are outlined in Table 1.

These commonly identified professional facilitators may use their professional positions or expertise to support serious financial crime activities in unique and varying ways:

- **Lawyers** can provide knowledge of tax law, company law and trust law, and advice on the use of company structures and trusts.
- **Accountants and financial advisers** often work closely with legal professionals to assist in concealing illicit wealth and advise on tax evasion strategies.
- **Liquidators and pre-insolvency advisers** may be used to facilitate illegal phoenix activities.
- **Offshore service providers** often work closely with legal professionals and can facilitate the creation of offshore corporate structures and associated bank accounts.<sup>10</sup>
- **Information and communications technology professionals** are critical to groups and individuals seeking to engage in financial crime who particularly require the use of technology, cybercrime and secure or encrypted communications practices.
- **Real estate agents** can facilitate the concealment of illicit wealth and money laundering through buying and selling high-value property.

In addition to these traditional professions that may facilitate serious financial crime, there are non-professional individuals who may be able to provide access to specialised knowledge, information or infrastructure, such as restricted datasets or computer systems, through their industry positions. These facilitators can provide expert opinion obtained from working within a particular sector or position regarding vulnerabilities that may be exploited to support serious financial crime.

## OUTLOOK

As outlined in *Organised Crime in Australia 2017*, serious and organised crime groups and individuals engaging in financial crime are likely to seek opportunities to increase illicit profits, avoid law enforcement detection, protect assets and conceal criminal wealth. Professional facilitators will continue to be fundamental in enabling financial crime, whether it is to launder funds or move money and/or assets offshore through complex financial structures or the exploitation of regulatory vulnerabilities.

## OFFSHORE SERVICE PROVIDERS

### INTRODUCTION

Offshore service providers (OSPs) facilitate the creation of offshore corporate structures and associated bank accounts as well as provide administration services, nominee directors or shareholders. These companies are often set up for legitimate tax minimisation purposes.

While the services offered by OSPs are legal, they are an attractive resource for serious and organised crime groups looking for ways to conceal beneficial (or true) ownership of assets and transfer illicit funds between jurisdictions. OSPs frequently use countries with strict secrecy provisions to incorporate companies, providing additional layers of anonymity.



### OFFSHORE SERVICE PROVIDERS KEY OBSERVATIONS

- Offshore service providers are likely to favour international jurisdictions that have a lower perceived risk and strong reputation for strict secrecy provisions, enabling additional levels of anonymity for their clients.

<sup>10</sup> More information is available in the next chapter 'Offshore service providers', which addresses the specific offshore services they provide to Australian citizens.

The anonymity afforded to clients of an OSP enables a range of criminal activity, including money laundering, and investment, superannuation and tax fraud. The use of multiple jurisdictions to register corporate entities, open bank accounts and hold assets can make investigation and disruption by law enforcement and regulatory agencies difficult, time consuming and expensive.

### CURRENT SITUATION

The use of OSPs to enable a range of serious financial crime is an ongoing issue. Investigations conducted under Project Wickenby uncovered widespread use of international OSPs to facilitate tax evasion and to conceal the beneficial ownership of a range of assets. OSPs continue to be used to create and administer offshore entities for the same purposes.

The publication of Mossack Fonseca client data has provided insight into the current extent to which Australian citizens and residents make use of OSPs. To date, over 1,000 entities have been identified as having used the services of Mossack Fonseca. However, while Mossack Fonseca was used to create offshore structures, the majority of Australian entities dealt with intermediaries in Australia or other jurisdictions, who in turn used Mossack Fonseca to register offshore entities. A number of clients were therefore not even aware that Mossack Fonseca was the entity that had registered their offshore entities. These layered arrangements can make it difficult to identify the beneficial ownership of corporate entities and associated assets.

While legitimate business people may be endeavouring to avoid or minimise tax, organised crime groups are more likely to use corporate structures created and administered by OSPs to hold funds derived from the sale of illicit commodities, as well as to return the funds to Australia to support an extravagant lifestyle and provide capital for legitimate investments.

### OUTLOOK

During the next two years, serious and organised crime groups and criminal individuals are likely to continue to use OSPs to maintain anonymity and facilitate criminal activity. The use of OSPs to create and administer offshore corporate entities is, and will almost certainly remain, legal. While OSPs provide a legitimate service, the existing legislation in many of the jurisdictions in which they operate provides scope for organised crime groups and individuals to exploit the system. It is also highly likely that many OSPs knowingly operate in a way that allows clients to conceal their identity and beneficial ownership of assets behind corporate structures.

The release of the Mossack Fonseca data, a growing recognition of the loss of taxation revenue and the exploitation of OSPs by a broad range of criminal groups has resulted in legislative change designed to restrict the criminal use of offshore corporate structures. The European Union has recently adopted changes to its anti-money laundering rules that will require each member state to maintain a public register showing the beneficial owners of companies and business-related trusts and enable the connection of these registers to facilitate cooperation between countries. Likewise, the United Kingdom has created a public register of the beneficial ownership of corporate entities.

Following the recent statutory review of Australia's anti-money laundering/counter-terrorism financing regime,<sup>11</sup> consideration is being given to legislative change designed to improve reporting requirements and enhance AUSTRAC's ability to capture financial intelligence related to the operation of OSPs.

A number of different models have been proposed, ranging from OSPs voluntarily registering with AUSTRAC to the use of domestic levers to compel registration or a requirement for Australian businesses to register offshore affiliates.

11 Attorney-General's Department 2016, *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations*, AGD, Canberra, viewed 2 May 2017, <<https://www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>>.

## ILLEGAL PHOENIX ACTIVITY

### INTRODUCTION

Illegal phoenix activity is ‘when a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements’.<sup>12</sup> Illegal phoenix operators have an unfair advantage when competing with other similar businesses because they accumulate debts they have no intention of repaying.

At its simplest, illegal phoenix activity involves running up debts in a company until it becomes insolvent and is placed into liquidation. The phoenix company is often a labour supply or employing entity with negligible assets and, once liquidated, the employees are transferred to a new company typically controlled by the same person or group.

### CURRENT SITUATION

Illegal phoenix activities divert money that should be afforded to the Australian revenue and tax systems to individuals through their businesses. Illegal phoenix activity results in employees not being paid the wages and superannuation to which they are entitled. Foreign workers are often exploited as part of the illegal phoenix activity.

Serious and organised crime groups have been identified as using illegal phoenix behaviour as a business strategy. Illegal phoenix activity is attractive to serious and organised crime groups partly due to the illicit profits that can be made by intentionally not paying goods and service tax, income tax or superannuation costs.

A current concern is the growth in the ‘pre-insolvency adviser’ market and its role in facilitating and promoting illegal phoenix activity. Unlike registered liquidators, pre-insolvency advisers operate in an unregulated environment. Some pre-insolvency advisers have been found to promote and facilitate illegal phoenix activities, for example by encouraging directors and accountants to transfer assets to new entities for less than market value, or to destroy or alter company records.<sup>13</sup>

<sup>12</sup> Australian Taxation Office, *Illegal phoenix activity*, viewed 2 May 2017, <<https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/>>.

<sup>13</sup> Australian Taxation Office 2016, *Phoenix Taskforce swoops on pre-insolvency industry*, viewed 18 July 2017, <<https://www.ato.gov.au/media-centre/articles/media-releases/phoenix-taskforce-swoops-on-pre-insolvency-industry/>>.



### ILLEGAL PHOENIX ACTIVITY KEY OBSERVATIONS

- The loss of tax and revenue caused by illegal phoenix activity has a negative impact on the Australian community as less money is available for community needs.
- The Australian Government has set in motion investigations and many modifications to the laws governing business to protect Australia from illegal phoenix activity.

There is no specific offence titled ‘illegal phoenix activity’ and this makes applying effective sanctions difficult, but there are applicable offences within the *Corporations Act 2001* that can be applied to the actions taken by directors and their advisers that result in illegal phoenix activity.

### PHOENIX TASKFORCE

The Australian Government is addressing illegal phoenix activity through information sharing, with government agencies working together on the multi-agency Phoenix Taskforce to identify those attempting to compromise the system. Through focused detection efforts, government agencies have increased the number of companies identified as using illegal phoenix behaviours.

### OUTLOOK

The ATO and ASIC experience demonstrates that phoenix operators and those who assist them are adaptable and, over time, become more deceptive and fraudulent. Regulators are responding to illegal phoenix models. Activities include not only enforcement, but disruption measures based on better market intelligence and an increasing use of data analytics to identify the high risk operators and their advisers.

# CASE STUDY

## PRE-INSOLVENCY ADVISERS LODGED FALSE DOCUMENTS WITH ASIC

An ASIC investigation culminated in charges being laid against two pre-insolvency advisers for lodging false documents with ASIC under a fictitious director identity. The fraud was undertaken to facilitate illegal phoenix activity by stripping assets from companies subject to liquidation.

The pre-insolvency adviser who created the fictitious identity was convicted of aiding and abetting the lodgement of false documents with ASIC and sentenced to six months imprisonment, suspended upon entering into a recognisance order to be of good behaviour for 12 months with a \$1,000 surety.

The pre-insolvency adviser's business partner—a chartered accountant who jointly ran the pre-appointment insolvency service—lodged the false and misleading documents appointing the fictitious identity as a company director with ASIC. The accountant was later convicted of this offence and sentenced to eight months imprisonment, to be served by way of an intensive correction order.<sup>i</sup>

<sup>i</sup> Australian Securities and Investment Commission 2015, *15-031MR Gold Coast chartered accountant sentenced following ASIC investigation*, media release, 19 February, ASIC, Canberra, viewed 3 May 2017, <[http://\\_asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-031mr-gold-coast-chartered-accountant-sentenced-following-asic-investigation/](http://_asic.gov.au/about-asic/media-centre/find-a-media-release/2015-releases/15-031mr-gold-coast-chartered-accountant-sentenced-following-asic-investigation/)>; Australian Securities and Investment Commission 2013, *13-356MR Former Gold Coast businessman pleads guilty to charges of creating a phantom company director and obstructing ASIC*, media release, 20 December, ASIC, Canberra, viewed 20 July 2017, <[http://\\_www.asic.gov.au/about-asic/media-centre/find-a-media-release/2013-releases/13-356mr-former-gold-coast-businessman-pleads-guilty-to-charges-of-creating-a-phantom-company-director-and-obstructing-asic/](http://_www.asic.gov.au/about-asic/media-centre/find-a-media-release/2013-releases/13-356mr-former-gold-coast-businessman-pleads-guilty-to-charges-of-creating-a-phantom-company-director-and-obstructing-asic/)>.



**ILLEGAL PHOENIX BEHAVIOUR  
IS A BUSINESS STRATEGY  
FOR ORGANISED CRIME**

Legislative changes go some way to addressing the problem. The *Insolvency Law Reform Act 2016* (the Act) modified the registration requirements for corporate insolvency practitioners to align with those of personal insolvency practitioners. Registered liquidators are no longer registered indefinitely, but instead must renew their registration every three years, in line with bankruptcy trustee registration requirements. The Act also introduced a new discipline process for registered liquidators.

Further, the Act increases ASIC's surveillance powers to review registered liquidator conduct, similar to the Australian Financial Security Authority's supervision of registered trustees. These initiatives, and the potential for further law reform, aim to mitigate the opportunity for illegal conduct and further improve integrity in the industry through enhanced options for addressing registered practitioner misconduct.

In September 2017, the Australian Government approved an initiative that would issue all Australian company directors with a unique Directors Identity Number. This initiative will provide a national reporting mechanism that enables government agencies to identify links between company directors and other companies and people that may be connected to illegal phoenix activity.

## ABUSIVE USE OF TRUSTS

### INTRODUCTION

Trusts are widely used for legitimate business and investment purposes,<sup>14</sup> including asset protection and tax liability reduction. The *abusive* use of trusts specifically refers to situations in which individuals have used trust structures to hide their control of a trust fund and extract wealth without being accountable for their tax obligations. An individual is able to control substantial assets using a trust structure. The control of those assets is often concealed by using a nominee or a trustee company whose officers and shareholders are not traceable. Individuals have exploited trusts to avoid or evade tax by concealing income, artificially reducing income and mischaracterising financial transactions.



### ABUSIVE USE OF TRUSTS KEY OBSERVATIONS

- Abusive use of trusts continues to contribute to revenue and tax fraud in Australia, with trust structures permitting individuals to effectively control significant wealth anonymously.
- There is scope for Australia to implement measures to promote transparency of beneficial ownership of trust funds, with indications that reforms may occur in the future.

### CURRENT SITUATION

The abusive use of trusts contributes to the overall total of revenue and tax fraud in Australia. Serious and organised crime groups and significant criminal individuals based in Australia and overseas have been identified as exploiting Australia's tax system through the abusive use of trust structures. Criminal groups and individuals use trust funds to conceal criminal wealth, support criminal activity and launder illicit funds.

The lack of transparency and the complexity inherent in legislative and regulatory frameworks surrounding trusts enable serious and organised crime groups and criminal individuals to conceal financial dealings using trust structures and provide anonymity to the beneficial owners.

Given the complexities of trust structures, there is an enhanced requirement to use professional facilitators. Tax agents, accountants and legal practitioners facilitate the creation, use and management of trusts; however, a small number of these same specialists have been identified as being noncompliant.

<sup>14</sup> Australian Taxation Office, *Trusts*, viewed 27 March 2017, <<https://www.ato.gov.au/general/trusts/>>.

# CASE STUDY

## ABUSIVE USE OF TRUST ACTIVITIES

The abusive use of trusts was employed to evade paying in excess of \$50 million in tax in the property development sector over a period of 10 years. It involved the siphoning off of profits from the main entities to trusts and companies controlled by the principal and their siblings, with these profits then being remitted offshore.

In some cases, completed properties were transferred below market value to related trusts, before being revalued to market prices and fully mortgaged, with the finance raised purportedly invested in a sham offshore property development syndicate. This had the effect of understating assessable profits, creating insolvency and recovery difficulties, and transferring wealth offshore without tax being paid. The case also involved related 'straw directors' (including offshore nominee directors), and raised doubts about the independence of appointed liquidators.



**TRUST FUNDS CAN BE USED TO  
CONCEAL CRIMINAL WEALTH,  
SUPPORT CRIMINAL ACTIVITY  
AND LAUNDER ILLICIT FUNDS**

## TRUSTS TASKFORCE

Professional facilitators who promote the misuse of trust structures were among those targeted by the former Trusts Taskforce.<sup>15</sup> Since its inception in 2013, the ATO-led Trusts Taskforce raised \$948 million in liabilities and collected \$279 million from individuals and businesses involved in tax evasion using trusts. An additional \$55 million worth of assets have also been restrained under proceeds of crime legislation.<sup>16</sup> Since 1 July 2017, the work of the Trusts Taskforce has continued under the ATO's Tax Avoidance Taskforce—Trusts.

Since the release of the Mossack Fonseca data, transparency and beneficial ownership, along with the role of professional facilitators, became particularly prominent issues for law enforcement, regulatory agencies and government. There is substantial overlap between trusts and offshore tax evasion.

## OUTLOOK

The revenue and tax fraud that occurs through the abusive use of trusts has an impact on the Australian community with the loss of government revenue resulting in less tax funds being available to spend on essential government services such as infrastructure, transport, health and education.

There is scope to improve the transparency of trusts in Australia. Early indications for change are noted in the Australian Minister for Justice's announcement at the United Kingdom Anti-Corruption Summit in May 2016, making a commitment to consult on options for a beneficial ownership register for companies. If measures recently implemented in other countries to improve corporate and trust transparency have an impact, similar reforms may occur in Australia. These reforms would go some way to increasing transparency of beneficial ownership, particularly measures relating to trusts, which would potentially reduce revenue and tax fraud in Australia.

## HIGH-VALUE COMMODITIES

### INTRODUCTION

High-value commodities continue to provide an effective vehicle for organised crime groups and criminal entities to commit financial crime.

<sup>15</sup> Australian Taxation Office 2017, *Trusts Taskforce*, viewed 27 March 2017, <<https://www.ato.gov.au/general/trusts/in-detail/compliance/trusts-taskforce/>>.

<sup>16</sup> *ibid.*



## HIGH-VALUE COMMODITIES KEY OBSERVATIONS

- Organised crime groups will continue to use high-value commodities as a way to exchange and conceal proceeds of crime.

They are used to store and transfer value and launder the proceeds of crime, due to the opportunity they afford to conceal illicit profits in legitimate assets that can be purchased with minimal regulatory oversight, and can over time accumulate ostensibly legitimate value.

High-value commodities include real estate, precious gems, valuable metals, art, antiquities, luxury vehicles and gold bullion. Gold bullion is not only used to store or transfer value but provides a way to exploit different tax treatments for gold and obtain fraudulent refunds.

## CURRENT SITUATION

### Australian real estate

The real estate sector in Australia is a strong investment vehicle for Australian and international investors. For those seeking to launder money or conceal proceeds of crime, the advantages of investing illegal profits in Australian real estate are that, not only is the value of investment likely to increase, the beneficial (true) ownership of the property can be concealed. In addition, professionals facilitating real estate transactions—such as real estate agents, conveyancers and lawyers—are not subject to most controls under Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime. They currently have no legal obligation to report suspicious transactions, despite these professions posing high money laundering/terrorism financing risks.<sup>17</sup>

<sup>17</sup> Attorney-General's Department 2016, *Report on the Statutory Review of the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and Associated Rules and Regulations*, AGD, Canberra, viewed 10 May 2017, <<https://www.ag.gov.au/Consultations/Documents/StatutoryReviewAnti-MoneyLaunderingAndCounter-TerrorismFinancingActCth200/report-on-the-statutory-review-of-the-anti-money-laundering.pdf>>.

**FIGURE 1: GOLD BULLION ENABLING GST FRAUD**



### Precious gems, valuable metals, arts and antiquities

Precious gems, valuable metals, art and antiquities also present opportunities for organised crime groups and criminal entities to transfer and store illicit wealth. Jewellery and precious gems in particular can be accepted within the criminal fraternity as a form of currency, where the transfer of value or the encashment of items are largely untraceable. The significant value of small items of jewellery and precious gems also enables more convenient storage, transfer and concealment than the equivalent value in cash. The goods are also free from reporting obligations when purchased using cash or when being moved out of Australia.

### Gold bullion

The high value of gold and its availability and portability provide significant opportunity for exploitation of the existing goods and services tax (GST) provisions, particularly in organised crime networks. GST fraud using gold bullion has been previously identified through the work of ATO Operation Nosean (see Figure 1). This type of fraud involved altering or misclassifying pure gold bullion and coins—which are not legally taxed—as lesser quality or scrap gold, which is taxed at 10 per cent, to fraudulently claim refunds in the form of GST tax credits.

This work of the ATO identified how valuable metals have created unique opportunities for criminal exploitation, but new government rules, enacted on 1 April 2017, require a reverse charge of GST to apply to all business-to-business taxable supplies of gold, silver and platinum, which places the onus on the purchaser of the valuable metal, not the supplier, to remit the GST to the ATO.

### OUTLOOK

Vulnerabilities in the AML/CTF framework have been highlighted as enabling criminal exploitation of high-value commodities. Focus has been placed on the current lack of reporting regulations for designated non-financial businesses and professions (DNFBPs), such as real estate agents, legal professionals and high-value dealers of valuable metals and precious gems—not including bullion dealers, who are regulated under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). The 2016 review of Australia's AML/CTF regime recommended that options be developed to regulate DNFBPs under the AML/CTF Act.

## ALTERNATIVE BANKING SERVICES

### INTRODUCTION

Alternative banking services (ABSs) are used by individuals and companies to move funds around the world outside existing regulated banking frameworks. ABSs generally offer low-cost international value transfers and virtually instantaneous delivery of funds.



### ALTERNATIVE BANKING SERVICES KEY OBSERVATIONS

- The use of alternative banking services currently appears to be more common in international jurisdictions than in Australia.

### CURRENT SITUATION

An ABS acts as an online banking interface that sits above and coordinates multiple bank accounts in various international locations. It provides a platform that hides the connection between the user of the service and any funds that are transferred, enabling members of the service to transfer value in a way that conceals the identity of the sender, recipient and beneficial owner. While the funds that enter the ABS account are pooled, the online banking platform provides the mechanism through which individual accounts within the ABS are managed.

Legitimate entities that favour these services include small businesses that operate transnationally, as they are attracted to the low transfer fees, which enable them to remain competitive, and geographically-dispersed families who need to transfer money in a timely manner. However, the anonymity that ABSs provide to clients also makes them attractive to serious and organised crime groups and criminal individuals. These criminal entities may exploit ABSs to enable a range of criminal activities including money laundering, tax evasion and various types of fraud.

### OUTLOOK

It is likely that ABSs will continue to provide a viable method for serious and organised crime groups and criminal individuals involved in financial crime to enable the movement of funds globally. However, the use of ABSs currently appears to be more common in international jurisdictions than in Australia.

# FINANCIAL CRIME MARKETS

## CYBERCRIME

### INTRODUCTION

Cybercrime is a crime committed directly or indirectly against a computer, system or network. Cybercrime actors are usually skilled individuals or groups who are engaged in the planning and execution of cyber intrusions. Cybercrime actors need not be physically co-located with others in their group, and are also often located overseas from their victims. Cybercrime methodologies and tools, including malware, are widely discussed and traded online.

Cybercrime is predominantly a financially-motivated crime that relies on the use of computers and communications technologies. The government's 2016 Cyber Security Review found cybercrime is costing the Australian economy up to \$1 billion in direct costs alone. Cybercrime against financial platforms and financial institutions is increasing, as is the sale of products and services that facilitate cybercrime. Cybercrime can be difficult to disrupt due to its highly technical nature, and due to cybercrime actors using a variety of anonymising techniques.

### CURRENT SITUATION

The global cybercrime market is a low risk, high return criminal enterprise. Cybercrime-related goods and services are highly sought after and are traded through online marketplaces and forums. Cybercrime actors targeting Australia for profit are predominantly based offshore. They are adaptable, resilient and sophisticated, and obscure their identities.

A number of different types of financially-motivated cybercrimes continue to pose a risk to the Australian public, the government, and businesses. These include credential-harvesting malware, ransomware, distributed denial of service extortion and Business Email Compromise.<sup>18</sup>



### CYBERCRIME KEY OBSERVATIONS

- Most entities involved in cybercrime target Australian victims and financial platforms from an overseas location.
- Cybercrime that seeks to generate significant profit continues to increase in both frequency and sophistication.

### CREDENTIAL HARVESTING MALWARE

Credential harvesting malware obtains legitimate account and/or login information, usually online banking login details. The malware is frequently delivered to a victim's computer through phishing emails containing malicious attachments. It can also be delivered through exploit kits hosted on malicious or compromised websites. When the malware is installed on a victim's device, it monitors and collects information, including bank account numbers and passwords, when the victim accesses an online banking platform. This information can then be used to make fraudulent payments or transfer money out of the victim's account.

Credential harvesting malware is designed to operate covertly, so it can remain undetected until the victim notices their money is missing. Credential harvesting malware can also be used to obtain logins and passwords to other systems, such as email, which can be used to send out spam and phishing emails.

<sup>18</sup> Australian Cyber Security Centre 2016, *2016 Threat Report*, ACSC, Canberra, viewed 3 May 2017, <[https://www.acsc.gov.au/publications/ACSC\\_Threat\\_Report\\_2016.pdf](https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf)>.

# CASE STUDY

## THIEVES USE MALWARE ON MOBILE PHONES TO STEAL BANK LOGIN DETAILS

In 2016, a credential harvesting malware strain was identified that targeted Australian mobile banking users. The malware displayed a false bank login page, when the victim attempted to access their mobile banking platform. This login page could not be bypassed and allowed cybercrime actors to obtain the victim's login details.

The cybercrime actors were then able to use the stolen credentials to log into a victim's account and transfer money out. The malware was also capable of stealing Google login information.<sup>i</sup>

<sup>i</sup> Tucker, H 2016, *Thieves have made a huge malware play to steal Australian bank login details on Android phones*, Business Insider Australia, Sydney, viewed 3 May 2017, <<https://www.businessinsider.com.au/thieves-have-made-a-huge-malware-play-to-steal-australian-bank-login-details-on-android-phones-2016-3>>.



**THE 2016 CYBER SECURITY  
REVIEW FOUND CYBERCRIME  
IS COSTING THE AUSTRALIAN  
ECONOMY UP TO \$1 BILLION**

## RANSOMWARE

Ransomware is a form of malware that stops a victim from using their computer or files until a sum of money is paid. Ransomware can either encrypt a person's files or lock a device, blocking access entirely. Ransomware usually targets a victim's computer via phishing emails or through malicious or compromised websites. In the 2016–17 financial year, ACORN received approximately 2,500 reports of ransomware targeting.

Successful ransomware campaigns in Australia use branding of trusted and well-known corporations as part of their social engineering techniques, as identified in the Australian Federal Police email case study.

## DENIAL OF SERVICE EXTORTION

A denial of service (DoS) is an attempt by a cybercrime actor to disrupt an individual or business by preventing legitimate access to online services (typically a website). This is achieved by flooding the targeted machine with requests, consuming the available bandwidth or the processing capacity of the computer hosting the online service.<sup>19</sup>

When multiple sources are used to flood an online service, usually coordinated through a botnet,<sup>20</sup> it is referred to as distributed denial of service (DDoS). Cybercrime actors can threaten an individual or company with a DoS or DDoS, unless a fee is paid. The actors may first conduct a short DoS/DDoS to demonstrate they have the capability to perform the attack, and to show the disruption it could cause.

## BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a criminal scheme targeting large and small businesses for financial gain. BEC traditionally involves 'spoofing' an identity, usually a high-level executive, in order to elicit payment. BEC is increasingly sophisticated, with attempts seemingly preceded by substantial research and preparation. BEC incidents are not always cybercrime and can be described as cyber-enabled crime.

Since the inception of ACORN in 2014, more than 2,000 reports of BEC have been registered with ACORN. BEC continues to have a substantial financial effect on Australia and internationally.

19 A DoS can also occur unintentionally through mis-configuration, or through a sudden and unexpected surge in legitimate usage.

20 A botnet is a number of internet-connected devices used by an owner to perform various tasks. The term most commonly has a malicious connotation.

## OUTLOOK

Australia's relative wealth and high uptake of social media and online services make it an attractive target for serious and organised crime groups and criminal individuals who use technology to facilitate their crime. Further, the increased use of technology in the financial sector both provides customers with convenient access to a range of services and presents increasing opportunities for technology-enabled fraud and cybercrime.

## INVESTMENT AND FINANCIAL MARKET FRAUD

### INTRODUCTION

Investment and financial market<sup>21</sup> fraud typically refers to the following types of criminal activities:

- fraudulent investment schemes, such as boiler-room fraud and Ponzi schemes, which attract victims with fake guarantees of high financial returns
- manipulation of the legitimate share market to artificially raise or lower the price of shares for financial benefit
- exploitation of financial securities,<sup>22</sup> such as fraudulent share schemes and off-market share transfers, and the use of margin lending facilities to make significant profit or launder the proceeds of crime.



### INVESTMENT AND FINANCIAL MARKET FRAUD KEY OBSERVATIONS

- Serious and organised crime groups rely on technology, identity crime and the use of professional facilitators to commit investment and financial market fraud.

21 The major markets in the Australian financial system are the credit market, stock market, money market, bond market and the foreign exchange market. Australian Bureau of Statistics, *Financial system*, viewed 4 May 2017, <<http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/by%20Subject/1301.0~2012~Main%20Features~Financial%20markets~267>>.

22 Financial securities on offer in Australia include shares, bonds, derivatives and managed funds.

# CASE STUDY

## RANSOMWARE IMITATING AUSTRALIAN FEDERAL POLICE EMAILS

A successful ransomware campaign seen in Australia involved emails imitating a traffic infringement from the Australian Federal Police. The potential victim receives an email stating that they have received an infringement that requires a fine to be paid. The email contains an attachment purporting to be photographic evidence of the offence being committed. If downloaded, ransomware is installed on the victim's computer, files are encrypted and payment is demanded for decryption.



**IN 2016–17, ACORN RECEIVED  
APPROXIMATELY 2,500 REPORTS  
OF RANSOMWARE TARGETING**

## CURRENT SITUATION

Australia is an attractive target for domestic and overseas-based serious and organised crime groups involved in investment and financial market fraud because of its comparatively stable economy, Australian investors' high subscription to share purchases, the perceived lower risk of detection and substantial illicit profits to be made.

The most recent reporting by the Australian Bureau of Statistics shows that approximately 1.6 million Australians experience personal fraud each year, at a combined personal cost of \$3 billion.<sup>23</sup>

In 2016, the Australian Competition and Consumer Commission experienced a 47 per cent increase in the number of scam reports from the previous year, and investment schemes accounted for the second highest amount of reported losses at \$23.6 million.<sup>24</sup> In 2016, ASIC received 367 reports about scams; however, the actual number of people affected by scams is likely to be much higher, as people often do not report that they have been scammed. The top five scams reported to ASIC are:

- overseas cold calling about investment opportunities
- overseas calls offering easy credit or loans after payment of an upfront fee
- sports arbitrage or gambling schemes
- money transfer schemes (job opportunity or other fraud)
- fake debt and invoice scams.

## FRAUDULENT INVESTMENT SCHEMES

Transnational and Australia-based organised crime groups and entities commit investment and financial market fraud against Australia through deceptive activities including boiler-room fraud and Ponzi schemes. In these fraudulent investment schemes, victims are pressured into investing funds with promises of high financial returns in a short period of time. However, victims end up losing most or all of their invested funds.

Boiler-room fraud or cold-calling investment fraud involves the unsolicited contacting of potential investors, who are deliberately given false or misleading information to entice them to buy, sell or retain securities or other investments.

A Ponzi scheme is an investment fraud where, unknown to the investors, there is no legitimate investment and returns are simply paid to investors out of money from subsequent investors.

This provides an appearance of legitimacy and gives investors the incentive to invest more of their own money and to encourage others to invest in the scheme. The scheme generally fails when either the criminal entities flee with all of the proceeds, insufficient new investors can be found, or the scheme is discovered by authorities.

These investment frauds can be delivered to a significant number of victims in any country over the phone or internet from any region in the world, using technology that can hide both the identity and the location of the perpetrators.

The groups that operate boiler-room fraud and Ponzi schemes use various tactics to make their schemes seem legitimate including aggressive telemarketing campaigns, glossy brochures, professional-looking websites—sometimes stealing the identity of legitimate companies<sup>25</sup>—and fake investment reviews. To maximise the success of these scams, professional facilitators are used to provide investment advice for use in cold-calling scripts, to provide fraudulent identification to open bank accounts, create companies, and set up internet accounts and professional-looking websites.

A range of different fraudulent investments are offered by scammers, including sports betting and gambling systems, securities schemes, superannuation schemes and foreign exchange trading.

In some cases, criminal entities set up online accounts for investors so they can see their balances rise, giving them the incentive to invest more money. However, investors soon realise they have been scammed when their requests to withdraw money are ignored and contact is cut off.

<sup>23</sup> Australian Bureau of Statistics 2016, *Personal Fraud*, viewed 4 May 2017, <<http://www.abs.gov.au/ausstats/abs@.nsf/mf/4528.0>>.

<sup>24</sup> Australian Competition and Consumer Commission 2017, *Targeting Scams*, viewed 18 July 2017, <[https://www.accc.gov.au/system/files/1162%20Targeting%20Scams%202017\\_FA1.pdf](https://www.accc.gov.au/system/files/1162%20Targeting%20Scams%202017_FA1.pdf)>.

<sup>25</sup> Government of Western Australia Department of Commerce Consumer Protection 2016, *2016 Scams Review: Losses and victimisation rates during 2016 for consumer fraud in Western Australia*, DCCP, Perth, viewed 9 May 2017, <[http://www.scamnet.wa.gov.au/scamnet/d/Resource\\_Library/CRE3OUHQKFLP9RA4BGM995X7BMJBYP/RJOJCTQY9WAQTZG.pdf/scamsreview2016.pdf](http://www.scamnet.wa.gov.au/scamnet/d/Resource_Library/CRE3OUHQKFLP9RA4BGM995X7BMJBYP/RJOJCTQY9WAQTZG.pdf/scamsreview2016.pdf)>.

# CASE STUDY

## INDIAN PENNY STOCK SCAM ON AN AUSTRALIAN STOCK EXCHANGE

In early 2017, ASIC detected the probable operation of a version of the Indian Penny Stock Scam on an Australian stock exchange.<sup>i</sup> The offshore service provider (OSP) running the fraudulent scheme listed offshore companies on an Australian exchange using initial shareholders who were all foreign citizens.

The share prices were often driven up by a single Australia-based broker executing very low volume trades. At the same time, these companies experienced an uncharacteristically significant amount of off-market transfers.

It is probable that the OSP was using the Australian exchange to create a reference price for their offshore company in Australia, from which off-market transfers were used as a vehicle to launder money and evade tax in foreign jurisdictions.

<sup>i</sup> The Penny Stock Scam in India involved large-scale money laundering and tax evasion through ramping up shares of small firms.



**TO AVOID BEING A VICTIM OF  
INVESTMENT FRAUD, INVESTORS  
SHOULD USE AUSTRALIAN  
STOCKBROKERS AND LICENSED  
FINANCIAL SERVICE PROVIDERS**

To reduce becoming a victim of investment fraud and increase the likelihood that investments are handled securely, investors should go through Australian stockbrokers and financial services providers licensed by ASIC. For investors wanting to deal with an overseas-based company that is not registered in Australia, it is recommended that investors visit the website of the International Organization of Securities Commission and check with the relevant authority where the overseas business is located, to confirm that they are appropriately registered to provide the services required.

### SHARE MARKET MANIPULATION

Criminal entities can manipulate or exploit the legitimate share market for significant financial gain. One way of doing this is through share market manipulation scams such as ‘pump and dump’ schemes, which involve the use of false and misleading information to generate investor trading interest to artificially ‘pump’ up the price of a company’s shares—normally a fraudulent or low value company. As more people invest, the share price increases and the scammers then sell or ‘dump’ shares at the peak of the price rise, giving them a considerable profit while causing the value of the shares to fall, leaving investors with shares that are either worthless or valued at a fraction of the purchase price.

### EXPLOITATION OF FINANCIAL SECURITIES

Criminal entities exploit financial securities to make illegal profits, such as through fraudulent share schemes (via boiler-room fraud), or to launder the proceeds of crime. For example, legitimate share markets can be exploited to launder illicit funds, as they provide investors levels of anonymity, particularly when trading through professional brokers.

Illicit funds can also be laundered through activities such as off-market share transfers, which involve the transfer of shares between parties without using a stockbroker. This practice can be exploited to launder illicit funds by using fraudulent identities to conduct off-market transfers of shares into false names.

ASIC has seen an increase in organised crime networks seeking to exploit offshore entities on the Australian share market, particularly in cases where no capital is raised in Australia and the majority of investors are offshore. These entities regularly have poor liquidity,<sup>26</sup> which organised crime networks exploit to transfer value or generate illicit profits.

### OUTLOOK

Investment and financial market fraud can distort Australia’s markets by diverting legitimate capital to non-productive or illicit investments. Such activity may reduce investor confidence in the integrity of these markets, with a consequent reduction in willingness to invest in legitimate entities. At the social level, such fraud causes financial hardship, reliance on welfare, mental illness or, in extreme cases, self-harm or suicide.

Australia will continue to be a target for domestic and offshore investment fraud activities. Law enforcement agencies, financial regulators and other bodies work independently and collaboratively across Australia to prevent and detect investment and market fraud in Australia.

## REVENUE AND TAXATION FRAUD

### INTRODUCTION

Revenue and taxation fraud involves the intentional abuse of the taxation system with the aim of obtaining financial benefit. It includes a number of noncompliant activities resulting in criminal penalties such as fines or imprisonment. These activities range from failing to report income in order to avoid taxation obligations to the use of complex offshore secrecy arrangements to evade tax.<sup>27</sup> Revenue and taxation fraud in Australia is made possible through the use of technology, identity crime and professional facilitators.

### CURRENT SITUATION

Organised crime groups, significant criminal individuals and some high-wealth individuals have been identified as committing revenue and tax fraud in Australia.

<sup>26</sup> Liquidity describes how easy it is to convert assets to cash.

<sup>27</sup> Australian Taxation Office 2015, *Tax crime explained*, viewed 6 April 2017, <[https://\\_www.ato.gov.au/General/The-fight-against-tax-crime/Tax-crime-explained/](https://_www.ato.gov.au/General/The-fight-against-tax-crime/Tax-crime-explained/)>.



## REVENUE AND TAXATION FRAUD KEY OBSERVATIONS

- Revenue and taxation fraud is committed by Australia-based crime groups but there are indications of offshore control of some syndicates committing refund fraud, offshore tax evasion and abusive use of trusts.
- Organised crime and other significant criminal individuals rely on technology, identity crime and professional facilitators to commit revenue and tax fraud.
- Revenue and taxation fraud has been committed through deceptive activities including illegal phoenix activity, abusive use of trusts, and the use of complex offshore secrecy arrangements.

While organised crime groups that commit revenue and tax fraud are primarily based in Australia, some syndicates who commit refund fraud, offshore tax evasion and abusive use of trusts are controlled by overseas-based entities.

### TAX REFUND FRAUD

Tax refund fraud occurs when people claim refunds, rebates or offsets that they are not entitled to. This can happen in a number of ways, from claiming fictitious expenses to creating false documentation to support a claim. Tax refund fraud is also committed when people dishonestly understate their income or provide false payment summary details, and when fraudulent tax returns are lodged using false or stolen identities. Identity crime related to refund fraud is an increasing problem.<sup>28</sup>

28 Australian Taxation Office 2015, *Refund fraud*, viewed 6 April 2017, <[https://\\_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Refund-fraud/](https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Refund-fraud/)>.

### OFFSHORE TAX EVASION

Globalisation and technological advances have made it easier for individuals to hold investments in offshore financial institutions, increasing the opportunity for tax evasion.<sup>29</sup> A high level of financial sector knowledge is required to successfully establish and operate large-scale fraud and tax evasion activities—this requires those committing the fraud to employ a professional to facilitate their activities. Facilitators include professionals in the accounting and law, money remittance, finance and insurance, import/export, and information and communications technology industries.

Project Wickenby, which targeted offshore tax evasion schemes, increased tax collections through improved compliance behaviour and enhanced the ability of Australian authorities to exchange information with other jurisdictions. The offshore tax evasion investigative work of Project Wickenby continues under the multi-agency Serious Financial Crime Taskforce.<sup>30</sup>

### ILLEGAL PHOENIX ACTIVITIES

Organised crime groups and other criminal individuals evade tax through illegal phoenix activities. Illegal phoenix activity occurs when ‘a new company is created to continue the business of a company that has been deliberately liquidated to avoid paying its debts, including taxes, creditors and employee entitlements’.<sup>31</sup>

### ABUSIVE USE OF TRUSTS

The abusive use of trusts contributes to revenue and tax fraud in Australia, with trust structures permitting individuals to anonymously control significant wealth. Serious and organised crime groups and significant criminal individuals have exploited trusts to avoid or evade tax by concealing income, artificially reducing income and mischaracterising financial transactions.

29 Australian Taxation Office 2015, *International tax crime*, viewed 6 April 2017, <[https://\\_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/International-tax-crime/](https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/International-tax-crime/)>.

30 Australian Taxation Office 2015, *Project Wickenby task force*, viewed 6 April 2017, <[https://\\_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Project-Wickenby-task-force/](https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Project-Wickenby-task-force/)>.

31 Australian Taxation Office, *Illegal phoenix activity*, viewed 6 April 2017, <[https://\\_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/](https://_www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Illegal-phoenix-activity/)>.

# CASE STUDY

## IDENTITY THEFT ENABLING TAX REFUND FRAUD

Over a two month period in 2010, a Thai national deceived three registered tax agents to lodge 217 fraudulent income tax returns with the ATO using stolen identities. The Thai national provided the tax agents with forged documents—provided by an associate in the fraud—which the tax agents accepted as genuine documents. The ATO detected the fraud as the unsuspecting individuals named in the fraudulent tax returns were not employed as reported. In March 2017, the offender was sentenced in New South Wales to three years jail for fraudulently claiming \$1.335 million in tax refunds.<sup>i</sup>

<sup>i</sup> Australian Taxation Office 2017, *Refund fraudster sentenced to three years jail*, viewed 19 April 2017, <[https://\\_www.ato.gov.au/Media-centre/Media-releases/Refund-fraudster-sentenced-to-three-years--jail/](https://_www.ato.gov.au/Media-centre/Media-releases/Refund-fraudster-sentenced-to-three-years--jail/)>.



**THE SERIOUS FINANCIAL CRIME  
TASKFORCE WILL CONTINUE TO  
TARGET, IDENTIFY AND CHARGE  
CRIMINALS WHO COMMIT  
REVENUE AND TAXATION FRAUD**

## EXPLOITATION OF TAX RULES IN RELATION TO VALUABLE METALS

Groups or networks of industry participants including refiners, bullion dealers, gold kiosks, dealers and buyers within established supply chains involved in gold recycling arrangements have been identified as seeking to exploit the goods and services tax (GST) rules in relation to valuable metals to fraudulently obtain GST refunds. As pure gold cannot be sold with the addition of GST, the fraud involves the seller melting or tarnishing the pure gold and selling the resultant scrap gold with the 10 per cent premium. Instead of remitting the GST to the ATO, the seller keeps the GST while the buyer claims a GST credit from the government. The buyer then recycles the scrap gold back into bullion, creating a 'carousel' in which GST payments are never sent to the ATO and GST credits are repeatedly claimed.<sup>32</sup>

To counteract this fraudulent activity, the Australian Government has introduced a new regulation that applies retrospectively from 1 April 2017. A 'reverse charge' of GST now applies to business-to-business taxable supplies of gold, silver and platinum, which places the onus on the buyer of the valuable metal, rather than the seller to remit the GST to the ATO.<sup>33</sup>

## OUTLOOK

The loss of government revenue from revenue and tax fraud has a flow-on effect for the Australian community, resulting in less tax revenue being available to spend on government services such as infrastructure, utilities, health and education.

Revenue and taxation fraud will remain a long-term issue in Australia as interactions between technology, identity crime and professional facilitators become increasingly complex and frequent. To address this issue, the Serious Financial Crime Taskforce and the ATO will continue to target, identify and charge organised crime groups and criminal individuals who commit revenue and taxation fraud.

32 Griffin, M 2017, 'Australia cracks down on gold industry tax fraud', *Sydney Morning Herald*, 2 April, [Online], accessed 18 April 2017, available at: <<http://www.smh.com.au/business/australia-cracks-down-on-gold-industry-tax-fraud-20170402-gvbvbq.html?deviceType=text>>.

33 Australian Taxation Office, *Reverse charge in the valuable metals industry*, viewed 18 April 2017, <<https://www.ato.gov.au/Business/GST/In-detail/Rules-for-specific-transactions/Reverse-charge-in-the-valuable-metals-industry/>>.

## SUPERANNUATION FRAUD

### INTRODUCTION

The superannuation industry in Australia primarily includes funds regulated by the Australian Prudential Regulation Authority (APRA), such as industry funds, corporate funds, retail funds and public sector funds, and self-managed superannuation funds (SMSFs), regulated by the ATO. As at June 2017, \$1,444.1 billion in superannuation assets were held by APRA-regulated superannuation funds while \$696.7 billion were held by SMSFs.<sup>34</sup>

### CURRENT SITUATION

Australia's large pool of superannuation funds is an attractive target for criminal groups and individuals.<sup>35</sup> The complex nature of superannuation schemes offers a range of opportunities for fraud including the theft of contributions and fund assets, fraudulent fund investments, non-existent schemes and excessive fees charged by advisers.<sup>36</sup>



## SUPERANNUATION FRAUD KEY OBSERVATIONS

- Superannuation fraud in Australia is made possible through the use of technology, cybercrime and identity crime.
- Self-managed superannuation funds are particularly vulnerable to exploitation by serious and organised crime groups and entrepreneurial criminals.

34 Australian Prudential Regulation Authority 2017, *Quarterly Superannuation Performance*, APRA, Sydney, viewed 12 September 2017, <<http://www.apra.gov.au/Super/Publications/Documents/2017QSP201706.pdf>>.

35 Australian Transaction Reports and Analysis Centre 2016, *Australia's Superannuation Sector: Money laundering and terrorism financing risk assessment*, AUSTRAC, Canberra, viewed 28 April 2017, <<http://www.austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB2.pdf>>.

36 National Organised Crime Response Plan 2015–2018.

## APRA-REGULATED SUPER FUNDS

APRA-regulated superannuation funds are susceptible to targeting by criminals, who are increasingly using technology, cybercrime and identity crime to commit superannuation fraud through activities such as hacking individuals' computers and using their personal identity information to fraudulently authorise the transfer of superannuation funds across to illegitimate SMSFs that are accessible to the criminal.

Early release scams are another form of superannuation fraud, where criminal entities offer super members access to their funds before the legal release age. Promoters of these illegal super scams often target people seeking debt relief, unemployed people and those from non-English-speaking backgrounds.

Victims' superannuation funds are rolled into a legitimate or illegitimate SMSF and are then stolen by the fraudster, or access to the funds is given to victims after a substantial fee is withdrawn for the criminal.<sup>37</sup>

Regulatory safeguards have been introduced to reduce the incidence of funds being illegally released from SMSFs. The ATO has improved the SMSF registration process to ensure only legitimate SMSFs are registered, and its new SMSF Member Verification System provides more certainty and transparency around rollovers from APRA-regulated super funds to SMSFs.

Penalties have also been introduced to prevent illegal early release of super funds. Promoters of illegal early release schemes face up to five years imprisonment, while those who access their superannuation benefits illegally will be taxed at the rate of 45 per cent on these amounts.

The accounts of members in APRA-regulated funds who have reached preservation age are particularly vulnerable to theft or fraud, as funds can be transferred in and out, like a bank account. The ability to withdraw funds from a superannuation account provides an opportunity for criminals to access these funds, if they can convince the account holder to invest in a fraudulent scheme.

APRA-regulated superannuation funds are responding to these vulnerabilities with the development of data analytic capabilities designed to detect unusual or suspicious activity. AUSTRAC also plays an important role in combating superannuation fraud by analysing reports received from industry pertaining to the use of fraudulent documentation in support of claims for early release of superannuation benefits, or death and disability insurance payments. AUSTRAC is sharing this intelligence with partner agencies for further investigation.

## SELF-MANAGED SUPERANNUATION FUNDS

Like APRA-regulated super funds, SMSFs also experience theft of contributions and fund assets. The growing balance of funds in SMSF accounts and the desire by individuals to choose and control their own investments make them particularly vulnerable to incidents of fraud.<sup>38</sup> For these reasons, individual SMSF account holders are especially vulnerable to becoming victims of superannuation fraud by organised crime groups and individuals through fraudulent fund investments, non-existent schemes and being charged excessive fees by SMSF advisers. Unlike APRA-regulated super funds, if an SMSF member loses money due to theft or fraud, they do not have access to any compensation schemes.<sup>39</sup>

Superannuation fraud is also committed when an SMSF contravenes the 'sole purpose test'. To meet the sole purpose test and be eligible for the tax concessions normally available to super funds, a trustee of an SMSF must ensure that the SMSF is maintained for the sole purpose of providing retirement benefits to its members, or to dependants if a member dies before retirement.

An SMSF fails the sole purpose test if the trustee provides a pre-retirement benefit to its members or anyone else, directly or indirectly—such as personal use of a fund asset.<sup>40</sup>

<sup>37</sup> Australian Securities and Investments Commission, *Superannuation scams*, viewed 27 April 2017, <<https://www.moneysmart.gov.au/scams/superannuation-scams>>.

<sup>38</sup> Drury, B 2015, 'Cyber gangs are targeting your super', *Sydney Morning Herald*, [Online], accessed 24 April 2017, available at: <<http://www.smh.com.au/money/super-and-funds/cyber-gangs-are-targeting-your-super-20150218-13igpg>>.

<sup>39</sup> Australian Securities and Investments Commission 2017, *Self-managed super fund (SMSF)*, viewed 27 April 2017, <<https://www.moneysmart.gov.au/superannuation-and-retirement/self-managed-super-fund-smsf>>.

<sup>40</sup> Australian Taxation Office 2017, *Sole purpose test*, viewed 17 July 2017, <<https://www.ato.gov.au/super/self-managed-super-funds/investing/sole-purpose-test/>>.

Contravening the sole purpose test is a tax crime that the ATO is carefully monitoring. In addition to an SMSF losing its tax concessions, trustees could face civil and criminal penalties.

## OUTLOOK

Losses to individual superannuation funds through fraudulent activities have the potential to increase financial hardship, causing a greater reliance on welfare payments and a loss of trust in the superannuation system.

The Australian Government introduced 'Stronger Super' reforms in 2012–13, which included measures to strengthen the governance, integrity and regulation of the Australian superannuation industry, particularly SMSFs. The reforms included giving the ATO powers to address wrongdoing and noncompliance by SMSF trustees, establishing a register of SMSF auditors (administered by the Australian Securities and Investments Commission), and making specialist knowledge and competencies mandatory for SMSF auditors and financial advisers providing services to SMSFs.<sup>41</sup>

## CARD FRAUD

### INTRODUCTION

Card fraud is the fraudulent acquisition and/or use of debit and credit cards or the card details. Card fraud may involve fraudulent applications, the theft of cards or card details, skimming of card details at automatic teller machines (ATMs), production of counterfeit cards, and phishing and hacking to obtain card details.

### CURRENT SITUATION

According to the Australian Payments Network, card-not-present fraud<sup>42</sup> continues to be the most prevalent type of fraud on Australian cards. Seventy-seven per cent of fraud on all Australian cards, perpetrated either in Australia or overseas in the 2015–16 financial year, is attributed to card-not-present fraud.<sup>43</sup>

41 The Treasury, *Stronger Super*, viewed 28 April 2017, <[https://strongersuper.treasury.gov.au/content/Content.aspx?doc=publications/government\\_response/key\\_points.htm#super\\_funds](https://strongersuper.treasury.gov.au/content/Content.aspx?doc=publications/government_response/key_points.htm#super_funds)>.

42 Card-not-present fraud occurs when valid card details are used to make purchases over the phone or internet—without the need for the card to be presented during the transaction—and without the authority of the card owner.

43 Australian Payments Clearing Association 2016, *APCA releases interim payments fraud data*, media release, 16 December, APCA, Sydney, viewed 19 March 2017, <[http://www.apca.com.au/docs/default-source/2016-Media-Releases/apca-](http://www.apca.com.au/docs/default-source/2016-Media-Releases/apca-releases-interim-payments-fraud-data.pdf)



## CARD FRAUD KEY OBSERVATIONS

- The global growth in technology in service delivery has presented expanding opportunities for organised crime, with card fraud being an increasing area of exploitation.
- The increase in online and cashless transactions suggests that the incidence of card-not-present fraud will also rise.
- Card fraud in Australia has frequently been undertaken by offshore crime groups that travel to Australia for the sole purpose of committing card fraud.

Over the five-year period from the 2010–11 financial year to the 2015–16 financial year, card-not-present fraud on all Australian cards increased from \$164 million to \$402 million respectively.<sup>44</sup> The rise in card-not-present fraud correlates with the increase in popularity of online shopping and the associated increase in the storage of these details online.

The intersection between smartphone technology and mobile payment platforms has enabled contactless payments using a smart device that contains linked credit card details. The rise in mobile payment services, which are intended to enhance customer convenience, follows the increasing use by Australians of smartphones to make online payments and purchases, and to access banking services.

[releases-interim-payments-fraud-data.pdf](#)>.

44 Australian Payments Network Limited 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015–30 June 2016*, Australian Payments Fraud Details and Data 2016, APNL, Sydney, viewed 25 August 2017, <<http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>>; Australian Payments Clearing Association 2011, *Fraud Statistics 2011 Financial Year Sheet - Payment Fraud Statistics 1 July 2010–30 June 2011*, APCA, Sydney, viewed 25 August 2017, <[http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2011-\(revised-december-2013\).pdf?sfvrsn=16](http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2011-(revised-december-2013).pdf?sfvrsn=16)>.

# CASE STUDY

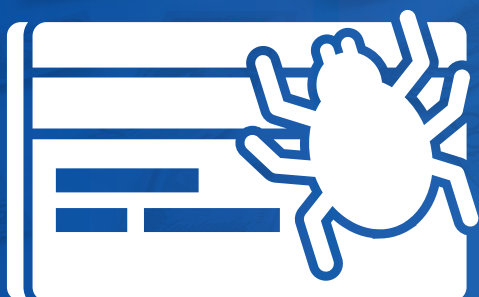
## CREDIT CARD DETAILS STOLEN AFTER HACK

In March 2017, a school photography company warned users of their online payment system that their website had been breached and the details of credit cards compromised. Users of the photography company reported that their credit cards had been used to pay for ride sharing, accommodation and airfares in Europe and the United States, with one user claiming there were charges of \$3,000 fraudulently attributed to their credit card.<sup>i</sup>

The website was reportedly compliant with Payment Card Industry Data Security Standards.<sup>ii</sup>

i Silva, K 2017, 'Hackers steal thousands after Queensland School Photography targeted online', Australian Broadcasting Corporation, Sydney, viewed 21 March 2017, <[http://\\_www.abc.net.au/news/2017-03-14/fraudsters-target-queensland-school-photos-stealing-thousands/8350502](http://_www.abc.net.au/news/2017-03-14/fraudsters-target-queensland-school-photos-stealing-thousands/8350502)>.

ii Branco, J 2017, *Credit card details stolen after school photographer's website hacked*, Brisbane Times, Brisbane, viewed 21 March 2017, <[http://\\_www.brisbanetimes.com.au/queensland/credit-card-details-stolen-after-school-photographers-website-hacked-20170313-guxcwj.html](http://_www.brisbanetimes.com.au/queensland/credit-card-details-stolen-after-school-photographers-website-hacked-20170313-guxcwj.html)>.



**CARD-NOT-PRESENT FRAUD  
ACCOUNTS FOR 77% OF FRAUD  
ON ALL AUSTRALIAN CARDS**

However, there are vulnerabilities in payment platforms that can be exploited by organised crime groups and tech-savvy criminals. Malware aimed at compromising smartphones may provide hackers with access to card details stored within mobile payment applications.<sup>45</sup> The 2015 ISACA Mobile Payment Security Study<sup>46</sup> identified the top four vulnerabilities of mobile payments as the use of public wi-fi, lost or stolen devices, phishing<sup>47</sup> or smishing,<sup>48</sup> and weak passwords.

While card skimming continues to occur, counterfeit/skimming fraud on Australian cards in Australia saw a negligible increase from the 2014–15 financial year (\$6.7 million) compared with the 2015–16 financial year (\$7 million).<sup>49</sup>

However, counterfeit/card skimming fraud on Australian cards overseas has seen a significant rise from \$17.1 million in the 2014–15 financial year to \$39.8 million in the 2015–16 financial year.<sup>50</sup> The rise of these types of card fraud is explained by Australian cards being compromised by fraud overseas in locations where preventative measures, such as chip technology, have not been as widely introduced as they have been in Australia.

Fraud on lost or stolen cards occurring either in Australia or overseas also increased from \$28.1 million in the 2014–15 financial year to \$34.3 million in the 2015–16 financial year<sup>51</sup> but still accounts for a small percentage of the overall card fraud on Australian cards.

## OUTLOOK

The harm experienced by individual victims of card fraud can range from inconvenience and reduced confidence in card security through to long-term effects on personal credit ratings, identity theft and compromising of privacy. While the impact of card fraud on the banking industry is felt through damage to reputation and disruption to services, any financial losses are most likely passed on to customers through increased fees and banking costs.

Australia is reported to be moving towards a cashless society that will be more reliant on mobile and contactless payment services.<sup>52</sup> Australia's use of cash will almost certainly decline in future, while debit and credit card transactions will continue to rise. Internationally, the movement towards a cashless society has seen an increase in online payment fraud and card fraud. It is likely that similar card fraud trends will be evidenced in Australia as contactless and mobile-based payment services are increasingly adopted.

45 Attorney-General's Department 2016, *Mazar malware attacking Android phones*, viewed 22 February 2016, <<https://www.staysmartonline.gov.au/alert-service/mazar-malware-attacking-android-phones>>.

46 ISACA 2015, *2015 Mobile Payment Security Study Global Results*, viewed 19 March 2017, <[http://www.isaca.org/SiteCollectionDocuments/2015-Mobile-Payment-Security-Study-Global-Data-Sheet\\_mis\\_Eng\\_0915.pdf](http://www.isaca.org/SiteCollectionDocuments/2015-Mobile-Payment-Security-Study-Global-Data-Sheet_mis_Eng_0915.pdf)>.

47 Phishing refers to identity theft tactics surrounding email and internet use.

48 Shmishing, also called smishing, refers to identity theft involving texts or short messages.

49 Australian Payments Clearing Association 2015, *Australian Payments Fraud; Details and Data 2015*, APCA, Sydney, viewed 19 March 2017, <<http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2015.pdf>>; Australian Payments Clearing Association 2016, *Australian Payments Fraud; Details and Data 2016*, APCA, Sydney, viewed 19 March 2017, <[http://www.apca.com.au/docs/default-source/fraud-statistics/australian\\_payments\\_fraud\\_details\\_and\\_data\\_2016.pdf](http://www.apca.com.au/docs/default-source/fraud-statistics/australian_payments_fraud_details_and_data_2016.pdf)>.

50 Australian Payments Clearing Association 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015-30 June 2016*, APCA, Sydney, viewed 25 August 2017, <<http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>>; Australian Payments Clearing Association 2010, *Fraud Statistics 2010 Financial Year Sheet - Payment Fraud Statistics 1 July 2009-30 June 2010*, APCA, Sydney, viewed 25 August 2017, <[http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-\(revised-december-2012\).pdf?sfvrsn=8](http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-(revised-december-2012).pdf?sfvrsn=8)>.

51 Australian Payments Clearing Association 2016, *Fraud Statistics 2016 Financial Year Sheet - Payment Fraud Statistics 1 July 2015-30 June 2016*, APCA, Sydney, viewed 25 August 2017, <<http://www.apca.com.au/docs/default-source/fraud-statistics/payment-fraud-statistics-financial-year-2016r.pdf>>; Australian Payments Clearing Association 2010, *Fraud Statistics 2010 Financial Year Sheet - Payment Fraud Statistics 1 July 2009-30 June 2010*, APCA, Sydney, viewed 25 August 2017, <[http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-\(revised-december-2012\).pdf?sfvrsn=8](http://www.apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2010-(revised-december-2012).pdf?sfvrsn=8)>.

52 Hunter, F 2016, 'Cashless future will save billions and requires red tape abolition: Alex Hawke', *The Canberra Times*, [Online], 17 February, accessed 14 June 2017, available at: <<http://www.canberratimes.com.au/federal-politics/political-news/cashless-future-will-save-billions-and-requires-red-tape-abolition-alex-hawke-20160216-gmv8ka.html>>.

# CASE STUDY

## BULGARIAN NATIONALS COMMIT CARD FRAUD IN AUSTRALIA

In March 2017, a Bulgarian national pleaded guilty to providing false documents and committing fraud as a result of participating in a card skimming ATM fraud with a fellow Bulgarian national. The two perpetrators attached skimming devices to the ATM, which recorded encrypted information about people's accounts, including their personal identification numbers. The information was then used to create new cards, which were used to make unauthorised cash withdrawals from the accounts. The individual entered Australia to commit the card fraud, departed and returned to commit further offences. The offender was sentenced to 3½ years prison and will be deported to Bulgaria at the completion of the sentence.<sup>i</sup>

i 'ATM fraudster to be jailed, then deported', *the Age*, [Online], 9 March 2017, accessed 19 March 2017, available at: <<http://www.theage.com.au/victoria/atm-fraudster-to-be-jailed-then-deported-20170309-guubv1.html>>; Cooper, A 2016, 'Bulgarians skimmed more than \$380,000 from Melbourne ATMs, court hears', *The Age*, [Online], 3 March, accessed 19 March 2017, available at: <<http://www.theage.com.au/victoria/bulgarians-skimmed-more-than-375000-from-melbourne-atms-court-hears-20160303-gn9kz1.html>>.

**CARD SKIMMING FRAUD ON  
AUSTRALIAN CARDS OVERSEAS  
ROSE FROM \$17.1M IN 2014–15  
TO \$39.8M IN 2015–16**

## HEALTH AND WELFARE FRAUD

### INTRODUCTION

Criminal groups and individuals are committing health and welfare fraud by exploiting vulnerabilities in government benefit and rebate frameworks, such as those that support family day care services. Sophisticated exploitation of health and welfare systems demonstrates a wide variety of criminal methodologies including collusion, the compromise of online systems and identity fraud.

Government revenue loss through fraudulent claims on health and welfare payments has the significant effect of reducing funds available for government services and programs, including legitimate health and welfare claims.

### CURRENT SITUATION

Entities and groups that are targeting government welfare, health and child support systems to commit fraud are predominantly opportunistic in nature. Many of the groups identified as perpetrating fraud are centred in communities that are geographically or culturally connected, or are businesses (such as medical practitioners or child care operators), rather than serious and organised crime groups.

That is not to say, however, that the welfare fraud being committed in Australia is not sophisticated, or that it does not target vulnerabilities in welfare programs in a systematic way. The Department of Human Services has identified an increasing number of cases in which the same individuals are committing fraud across a number of programs or using deceptive practices that demonstrate a level of sophistication.

Investigations or compliance activities into fraudulent claims for or overpayment of associated Commonwealth benefits may discover information relating to other types of health and welfare fraud. Individuals involved in one type of health and welfare fraud often seek to exploit vulnerabilities in other Commonwealth benefits schemes. For example, educators and parents involved in family day care fraud often receive other Commonwealth benefits, including Newstart and youth allowances, and single parent and disability support pensions. While there may be legitimate claims to a number of Commonwealth benefit schemes, the involvement in one type of health and welfare fraud increases the likelihood of being involved in other types of Commonwealth benefit fraud.



### HEALTH AND WELFARE FRAUD KEY OBSERVATIONS

- Health and welfare fraud is predominantly an opportunistic crime carried out by people with both access to and knowledge of health and welfare services and systems.
- Serious organised crime groups have not traditionally been involved in this type of financial crime.
- Health and welfare fraud is anticipated to grow in line with the increased migration of government services to online platforms.

Taskforce Integrity, a joint operation between the Department of Human Services and the AFP, targets geographic locations with a higher risk of welfare fraud and noncompliance. The task force aims to change localised cultures of noncompliance and positively influence customer behaviour by encouraging self-correction. The activities of Taskforce Integrity range from individual compliance reviews through to investigations of organised and complex fraud.

A factor compounding the prevalence and scale of this type of fraud is that the child care benefit and child care rebate programs are provided by Australian Government departments, while compliance with the conditions of the programs are administered by the state and territory departments of education.

While the majority of health, welfare and child support frauds against Australian welfare systems have been undertaken domestically, it is anticipated that the targeting of online government portals will increase and that these systems may possibly be breached by offshore entities.

### OUTLOOK

Health and welfare fraud has a genuine negative impact on government revenue, reducing the funds available to allocate to government services and programs. The theft of medical records, tax information or personal identifying information, with a view to use in defrauding the government of welfare, health and/or child support payments, also has a personal impact on the victims of this identity theft.

# CASE STUDY

## EXPLOITATION OF SCHEME FOR VULNERABLE CHILDREN IN CHILD CARE FRAUD

Between September 2013 and March 2015, a child care centre was identified as charging families with children in care approximately \$9,000 per week, including 14 at-risk children, in order to exploit the government rebate for the Special Child Care Benefit. No invoice was given to the parents as the child care provider received 100 per cent of the claimed benefit.

This scam defrauded the government of \$3.6 million—one of the largest child care frauds in Australia. The charges laid against the child care operator included 66 counts of dishonestly obtaining financial advantage by deception, 15 counts of using forged documents and one count of dealing with money and property believed to be proceeds of crime worth more than \$1 million.

The child care provider was sentenced to seven years in prison.<sup>i</sup>

<sup>i</sup> Balogh, S & Morton, R 2017, 'Seven years' jail after taxpayers footed bill for \$3.6m childcare rort', *The Australian*, [Online], 27 May, accessed 16 June 2017, available at: <<http://www.theaustralian.com.au/news/nation/seven-years-jail-after-taxpayers-footed-bill-for-36m-childcare-rort/newsstory/2703cec51163ddcc045fa6a1a3e4e5d2?nk=17472f53799716159c71d6ee21428a07-1496197212>>.



**THOSE INVOLVED IN HEALTH  
AND WELFARE FRAUD  
OFTEN SEEK TO EXPLOIT  
VULNERABILITIES IN  
MULTIPLE COMMONWEALTH  
BENEFITS SCHEMES**

# FINANCIAL CRIME OUTLOOK IN AUSTRALIA

Serious and organised crime group involvement in financial crime has been assessed as being likely to continue to increase during the next two years. Similarly, it is almost certain that individuals with significant wealth and/or intent to engage in serious financial crime will exploit vulnerabilities in processes and frameworks of the financial sector, government programs, regulatory environments and reporting requirements.

## KEY PREDICTIONS

Money laundering investigations undertaken across Australia have led to an enriched intelligence picture of serious financial crime. The strategic picture suggests that those involved in money laundering use multiple methodologies, and that law enforcement attention to one methodology leads to displacement to alternative methodologies—some of which are better understood than others. Money laundering will continue to pose a threat, but the significant change will be in the identified methodologies used by international money laundering organisations to transfer and conceal illicit funds globally.

Though the role of technology in enabling financial crime has been on the rise for some years, recent years have seen a marked escalation in its use.

Similarly, the risk posed by cybercrime, while not new, has increased rapidly and is now recognised by the financial sector as a primary ongoing area of risk. The use of technology to enable financial crime, and the risk posed by cybercrime, will continue to grow.

The release of Mossack Fonseca client data and similar datasets, which include information on Australian entities, has shown that the extent of tax evasion facilitated by large corporate offshore service providers is likely to be considerably larger than previously thought. Investigating the role of offshore service providers in facilitating this financial crime will be a priority for Australian law enforcement and partner agencies over the next two years.

A whole-of-government focus on the collection of intelligence in relation to the role of professional facilitators will support quantifying and qualifying the role that they play in enabling financial crime. It is anticipated that, as the integration of technology in government and financial service delivery expands, the services of professional experts to facilitate financial crime through these e-platforms will also increase. Similarly, as governing rules of superannuation, investment and financial market frameworks change, professional advice to identify and exploit loopholes will also be increasingly sought out. Professional facilitators will continue to offer a degree of expertise, insulation, access and efficiency that is integral to serious financial crime activities.

## OPPORTUNITIES

The Australian Government is taking a holistic approach to tackling serious financial crime. Initiatives combining the strengths of government agencies with a financial crime remit, coupled with industry and community collaboration, are generating prevention and response opportunities.

Targeting enablers of financial crime provides a unique opportunity to affect illicit markets. The impacts of law enforcement, regulatory, legislative or policy activity to disrupt enabling activities have the potential to resonate through all illicit markets in which those enabling activities are present. For example, should law enforcement agencies' capability to identify, trace and prosecute technology-enabled financial crime be enhanced, all markets that rely on technology to perpetrate crime would be significantly affected.

Similarly, if policy, legislative or regulatory changes are implemented in markets or against enablers relevant to serious financial crime, then it stands to reason that these changes would also have an impact across other crime types and markets, particularly where there is a nexus with financial crime, such as terrorism financing.

Intelligence collection and investigative actions of the Serious Financial Crime Taskforce will continue to deliver an informed intelligence picture and evidence base of the nature and extent of the risks that the highest priority financial crimes present to Australia. This evidence base will assist to inform any policy, legislative and/or regulatory change required to not only disrupt financial crime but to also make the environment more adverse and resistant to those looking to engage in financial crime in Australia.

While financial crime will continue to pose a real risk to Australia, the work of the Serious Financial Crime Taskforce will continue to provide opportunities to understand and respond agilely to that risk.

---

# ACRONYMS

<b>ABF</b>	Australian Border Force
<b>ABS</b>	Alternative banking service
<b>ACIC</b>	Australian Criminal Intelligence Commission
<b>ACORN</b>	Australian Cybercrime Online Reporting Network
<b>AFP</b>	Australian Federal Police
<b>AGD</b>	Attorney-General's Department
<b>AML/CTF</b>	Anti-money laundering/counter-terrorism financing
<b>APRA</b>	Australian Prudential Regulation Authority
<b>ASIC</b>	Australian Securities and Investments Commission
<b>ATM</b>	Automatic teller machine
<b>ATO</b>	Australian Taxation Office
<b>AUSTRAC</b>	Australian Transaction Reports and Analysis Centre
<b>CDPP</b>	Commonwealth Director of Public Prosecutions
<b>DNFBP</b>	Designated non-financial businesses and professions
<b>DoS/DDoS</b>	Denial of service/Distributed denial of service
<b>GST</b>	Goods and services tax
<b>ICT</b>	Information and communications technology
<b>OSP</b>	Offshore service provider
<b>PII</b>	Personal identifying information
<b>SMSF</b>	Self-managed superannuation fund
<b>SVC</b>	Stored value card
<b>TBML</b>	Trade-based money laundering



Discovering threats,  
supporting law enforcement,  
protecting Australia.

[www.acic.gov.au](http://www.acic.gov.au)